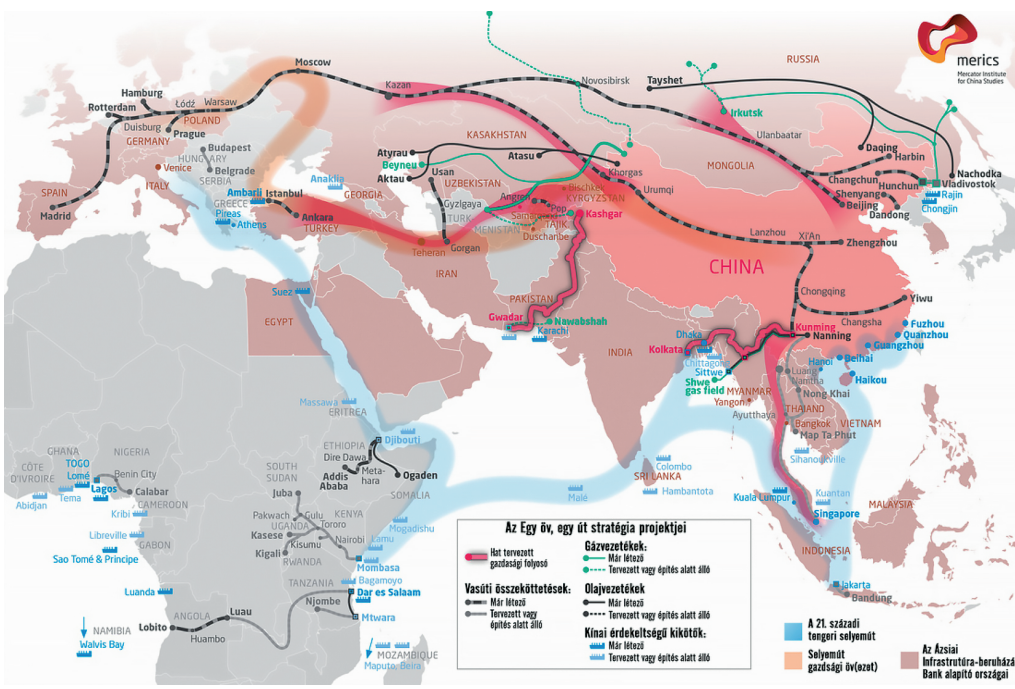
5. Napjaink (új típusú) kihívásai, kockázatai és fenyegetései

5.1. Bevezetés

A világ problémáinak átfogó elemzése megköveteli, hogy a diplomáciai, gazdasági, katonai és információs területeket egyaránt figyelembe vegyük (*diplomatic, information, military, economic* – DIME), hiszen ezek a dimenziók szorosan összefonódnak, és kölcsönösen befolyásolják egymást. A diplomáciai kapcsolatok elemzése segít megérteni az államok közötti viszonyokat, a szövetségek és konfliktusok dinamikáját, valamint a nemzetközi együttműködés lehetőségeit. A gazdasági tényezők vizsgálata rávilágít az országok közötti kereskedelmi kapcsolatokra, a gazdasági növekedés és stabilitás kérdéseire, valamint a globális piacok alakulására. A katonai szempontok elemzése elengedhetetlen a biztonsági kihívások és a fegyverkezési verseny megértéséhez, míg az információs terület vizsgálata feltárja a dezinformációs kampányok, a kiberbiztonság, az információs hadviselés és a mesterséges intelligencia jelentette veszélyeket. Csak ezen területek integrált elemzésével kaphatunk reális képet a ránk váró stratégiákról, kihívásokról, kockázatokról és fenyegetésekről, ami elengedhetetlen a hatékony döntéshozatalhoz és a proaktív válságkezeléshez. Az elemzések által lehet egy ország ellenálló képességét (reziliencia) tovább fejleszteni és megfelelni a jövő kihívásainak.

A világ hatalmi rendszerének jelentős változása és a világ újrafelosztása zajlik, emellett a világ erőforrásaiért is rendkívül nagy a vetélkedés és a nyomásgyakorlás (lásd ukrán ritka földfémek).

A gazdasági térben az országok újrarendeződése látható (BRICS-országok), továbbá egy világhatalom (Kína) tervezi az *Egy övezet egy út* geostratégiai terv megvalósítását. A terv lényege az erőforrások megszerzése, a geostratégiailag fontos szűk keresztmetszetek (átjárók, szorosok, kikötők, szárazföldi csomópontok) uralma és használata a kínai termékek gyors és akadálymentes eljuttatása érdekében a világ bármely pontjára, felhasználva az orosz energiahordozókat a gyártáshoz *(10. ábra).*



10. ábra: A kínai egy övezet egy út geostratégiai projektjei
Forrás: Horváth 2020

DOI: https://doi.org/10.36250/01319_05

5.1.1. Az EU

Az Európai Unió jelenlegi helyzete több kihívással is szembesül, amelyek közül az egyik legjelentősebb a gazdasági versenyképesség kérdése. Az EU gazdasági teljesítménye elmarad az Amerikai Egyesült Államok és Kína dinamikus növekedésétől, ami részben az innovációs beruházások hiányára és a belső piaci szabályozások komplexitására vezethető vissza. Emellett demográfiai problémák is sújtják a régiót, hiszen az elöregedő népesség és a csökkenő születésszám hosszú távon veszélyezteti a munkaerőpiac stabilitását és a szociális rendszerek fenntarthatóságát. Az illegális migráció további terheket ró az Unióra, mivel a bevándorlók integrációja gyakran nehézségekbe ütközik, és a tömeges migrációval összefüggő bűnözési és terrorcselekmények kérdései fokozzák a társadalmi feszültségeket. Az EU-nak sürgős reformokra van szüksége, hogy megerősítse gazdasági pozícióját, kezelje a demográfiai kihívásokat, és hatékonyabban irányítsa a migrációs folyamatokat.

Az Európai Unió az ukrajnai konfliktus kezdete óta (2022. február 24.) elkötelezetten támogatja Ukrajnát, különösen a fegyverszállítások és a védelmi képességek erősítése terén. Az EU tagállamai közösen dolgoznak azon, hogy növeljék a lőszergyártást és felpörgessék a hadiipari termelést, ezzel biztosítva, hogy Ukrajna megfelelő haditechnikai eszközökkel rendelkezzen területi integritásának védelméhez. A fegyverszállítások mellett az Unió technikai, logisztikai pénzügyi és menekültügyi támogatást is nyújt, valamint szorosan együttműködik a NATO-val és más nemzetközi partnerekkel a hatékony segítségnyújtás érdekében. Az EU hangsúlyozza a konfliktus diplomáciai megoldásának fontosságát, de a béketervek ellenére úgy gondolja, hogy a jelenlegi helyzetben elengedhetetlen a katonai támogatás, hogy Ukrajna megvédhesse szuverenitását és a nemzetközi jog által biztosított jogait.

5.1.2. A NATO

A NATO globális szerepe az elmúlt években egyre hangsúlyosabbá vált, különösen a Közel-Kelet és a Távol-Kelet vonatkozásában. Iránnal mint középhatalommal szemben a NATO célja a regionális stabilitás fenntartása és a nukleáris fegyverek elterjedésének megakadályozása. A Vörös-tenger biztonsága, amelyet a jemeni lázadók tevékenysége is fenyeget, szintén figyelmet kap a szabad tengeri kereskedelem és a szabad hajózás biztosításához. A NATO szorosan figyelemmel kíséri a Tajvan körüli feszültségeket is, hiszen a térség stabilitása globális gazdasági és biztonsági érdekeket érint. A szövetség célja, hogy erősítse a nemzetközi együttműködést, a nemzetközi jog tiszteletben tartását és támogassa a békés megoldásokat. Az ukrajnai konfliktus kapcsán a NATO jelentős segítséget nyújt Ukrajnának, beleértve a haditechnikai eszközök átadását, a lőszergyártás támogatását, valamint az ukrán katonák kiképzését (119 milliárd USD). Különösen fontos a légvédelemi és a tüzérségi rendszerek fejlesztése, amelyek kritikusak Ukrajna védelmi képességének növelésében.

Az európai NATO-országok védelmi kiadásai az elmúlt években növekedtek (2%), de még mindig elmaradnak az Egyesült Államok szintjétől (3,36%). Az USA jelentős mértékben hozzájárul a NATO költségvetéséhez és katonai kapacitásaihoz, ami biztosítja a szövetség globális jelenlétét és gyors reagálóképességét, az erő kivetítésének lehetőségét. Az európai országok fokozatosan növelik védelmi kiadásaikat a közös biztonsági célok elérése érdekében, de néhány ország számára továbbra is kihívást jelent a 2%-os GDP-arányos védelmi költségvetési cél elérése, amelyet a NATO tagjai vállaltak. Az amerikai védelmi kiadásokhoz viszonyítva az európai

hozzájárulások kisebbek, de a transzatlanti együttműködés és az erőforrások megosztása révén a NATO továbbra is hatékonyan képes kezelni a globális biztonsági fenyegetéseket. A USA elvárása, hogy a NATO-országok tovább növeljék védelmi kiadásaikat, esetleg 3-5%-ra.

Az Amerikai Egyesült Államok atomfegyverei kulcsszerepet játszanak az ország nemzetbiztonsági stratégiájában, valamint a globális elrettentés fenntartásában. Az USA elkötelezett az atomfegyverek elterjedésének megakadályozása mellett, amelyet nemzetközi egyezmények keretében valósít meg. Az Egyesült Államok aktívan részt vesz a fegyverzet-ellenőrzési tárgyalásokban és kezdeményezésekben, hogy korlátozza a nukleáris arzenálok méretét, és elősegítse a globális biztonságot azzal, hogy megakadályozza egyes országok képességeinek kifejlesztését. Az USA számára fontos, hogy megakadályozza Irán nukleáris fegyverekhez jutását, amely célkitűzést diplomáciai eszközökkel és gazdasági szankciókkal támogatja. Az orosz nukleáris arzenál ellensúlyozása érdekében az USA fenntartja saját stratégiai nukleáris képességeit, amelyek elegendőek a kölcsönös elrettentés biztosításához. Bár az orosz arzenál mérete jelentős (5580 darab), az Egyesült Államok (5044 darab) technológiai fejlettsége és szövetségesi rendszere révén képes fenntartani az erőegyensúlyt, és biztosítani, hogy a nukleáris fegyvereket ne vessenek be. Az atomfegyverek alkalmazása a modern világban gyakorlatilag elképzelhetetlen, hiszen a nukleáris fegyverek használata globális katasztrófához vezetne, amelyet minden nemzet igyekszik elkerülni. Az Amerikai Egyesült Államok mint a világ egyik legnagyobb nukleáris hatalma kulcsszerepet játszik Európa biztonságának garantálásában. Egyedül az USA nukleáris elrettentő képessége biztosítja a kölcsönös megsemmisítés doktrínáját, amely szerint bármilyen nukleáris támadás azonnali és teljes mértékű válaszcsapást vonna maga után, ezzel elrettentve Oroszországot vagy bármely más hatalmat attól, hogy nukleáris fegyvereket vessen be. Az Egyesült Államok védelmi és diplomáciai erőfeszítései, valamint NATO-szövetségeseivel való szoros együttműködése révén képes fenntartani a stabilitást és a békét Európában, megakadályozva, hogy egy ilyen pusztító háború valaha is kitörjön.

Magyarország biztonsági helyzetét a NATO- és EU-tagságunkból adódóan a stabilitás, a fejlődés határozza meg. Folyamatosan változó világunkban az ország nemzeti érdekeinek védelme, fejlődésének biztosítása és a Magyar Honvédség feladatainak meghatározása nem egyszerű feladat. Forrongó világ, gyorsan változó helyzetek határozzák meg nemzeti céljainkat. A globális térben zajló biztonság- és védelempolitikai folyamatok hatásaiból a szomszédunkban három éve folyó háborút, a tömeges illegális migrációt, a közel-keleti terrorizmust és a tömegpusztító fegyverek elterjedésének a veszélyét (proliferáció) kell kiemelni.

Magyarország biztonságát számos pozitív tényező erősíti, amelyek közül kiemelkedik a NATO- és EU-tagság, hiszen ezek a szervezetek szilárd keretet biztosítanak az ország védelmi és gazdasági stabilitásához. A NATO-tagság garantálja a kollektív védelem előnyeit, míg az EU-tagság gazdasági és politikai támogatást nyújt. A regionális együttműködés, különösen a visegrádi négyek (V4) keretében, lehetőséget ad a közös politikai, gazdasági érdekek érvényesítésére és a közép-európai térség biztonságának erősítésére. Magyarország haderőfejlesztési programja szintén hozzájárulnak a védelmi képességek korszerűsítéséhez és az ország biztonságának fokozásához, munkahelyek teremtéséhez. Az illegális migráció megakadályozása szintén kulcsfontosságú a határok védelme és a belső stabilitás fenntartása szempontjából. Magyarország biztonságát negatívan befolyásolják a szomszédunkban folyó háború, a demográfiai kihívások, mint az elöregedő népesség és a csökkenő születésszám, amelyek hosszú távon fenntarthatósági kérdéseket vetnek fel. Az infláció és az államadósság szintén gazdasági instabilitást okozhatnak, ami közvetett módon befolyásolja az ország biztonsági helyzetét. A komplex kihívások kezelése érdekében Magyarországnak kiegyensúlyozott és átfogó stratégiát kell alkalmaznia, amely figyelembe veszi mind a pozitív, mind a negatív tényezőket.

5.2. Elméleti alapok

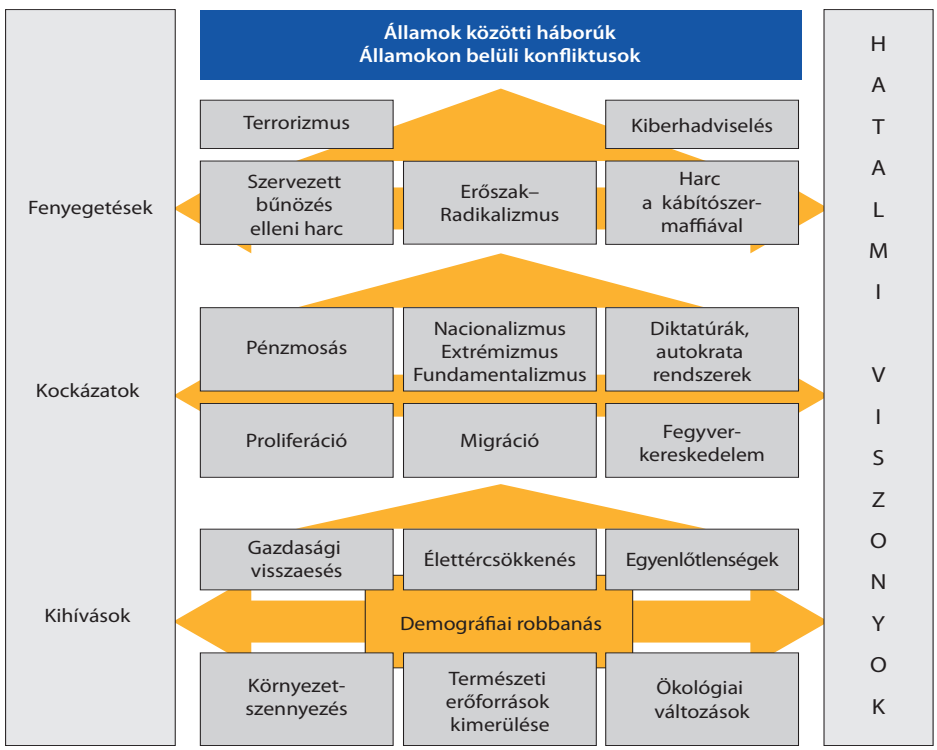
A biztonságpolitikai és nemzetbiztonsági kihívások, kockázatok és fenyegetések általában azok a helyzetek és állapotok, amelyek negatív hatással vannak a biztonság egyes dimenzióira. Tekintsük át a fogalmakat!

Fogalmak

A kihívások: az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek legalacsonyabb megnyilvánulási szintjén, amelyek eredői általában hátrányosan befolyásolják a belső és külső stabilitást, és hatással lehetnek egy adott régió hatalmi viszonyaira.

A kockázatok: az általánosan értelmezett biztonság egyes összetevőire ható helyzetek és állapotok összessége a lehetséges veszélyek olyan megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek.

A fenyegetések: az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek legmagasabb megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, és közvetve hatással lehetnek a nemzeti értékek megőrzésére.



11. ábra: A kihívások, kockázatok és fenyegetések
Forrás: Resperger István (2002): *A fegyveres erők megváltozott feladatai a katonai jellegű fegyveres válságok kezelése során.* Doktori értekezés. Budapest: ZMNE.

Az érdekek képviseletének módszerei és eszközei előnyben részesítik a kikényszerítést vagy az erőszakos úton történő megoldás lehetőségét. Amint az a fogalmi meghatározásokból kitűnik, a kihívásokat, a kockázatokat és a fenyegetéseket a lehetséges veszélyek megnyilvánulási formáinak tekintem, amelyek általában hátrányosan befolyásolják a belső és külső stabilitást, és hatással lehetnek egy adott régió hatalmi viszonyaira. Ezek a fogalmak intenzitásuk szerint egymásra épülve jeleníthetők meg, egyre nagyobb feszültségi szint meglétét feltételezve. Jellegükből következően csak dinamikus folyamatokként értelmezhetők, ezért a fogalmi meghatározások az elméleti értelmezés szempontjából fontosak, de gyakran egymással átfedésben, összemosódva jelennek meg, és a külső környezeti jellemzők (például a politikai, gazdasági viszonyok) függvényében képlékenyen változhatnak.

5.3. Konfliktussal, konfliktusmegelőzéssel, válsággal, válságkezeléssel kapcsolatos elméleti alapok

A témával kapcsolatos fogalmakat, meghatározásokat és definíciókat az államközi kapcsolatok viszonyának formáin keresztül közelítem meg. A szakirodalom alapvetően az esetek többségében négy állapotot különböztet meg:

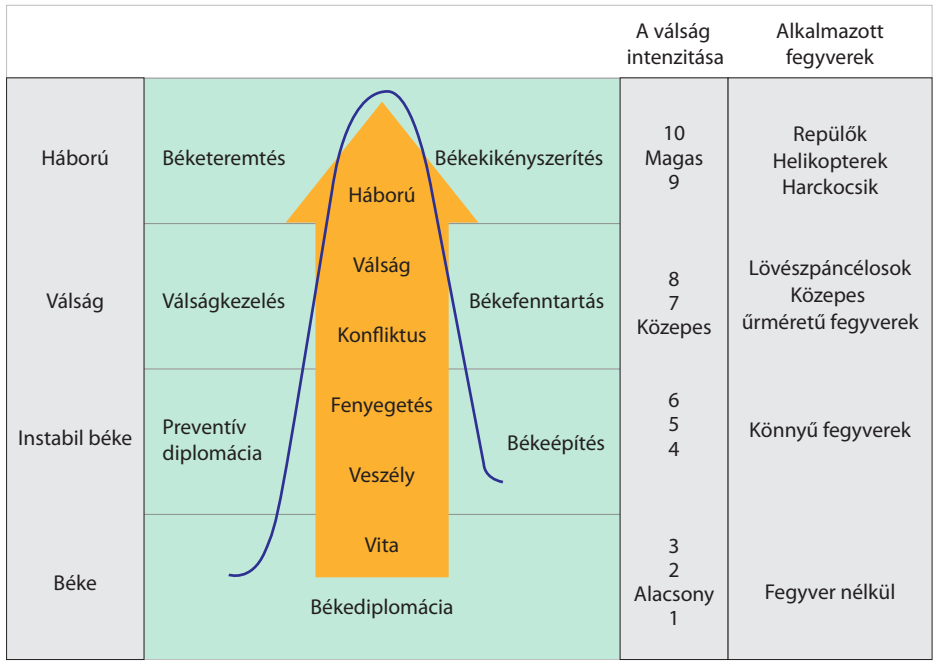
- békeállapot;
- válsághelyzet;
- katonai természetű veszélyeztetés;
- konfliktuskezelés utáni békeállapot.

A *békeállapot* jellemzője, hogy az államok és/vagy az országcsoportok közötti kapcsolatok a kölcsönös bizalmon és az egyetértésen alapulnak a közös érdekek és a valós értékek figyelembevételével.

A *válsághelyzet* jellemzője, hogy a jó kapcsolat valamilyen vita vagy érdek-, illetve értékütközés következtében megromlik, feszültség keletkezik a résztvevők között, akik valamilyen (politikai, diplomáciai, gazdasági, katonai) eszközzel megpróbálják a kialakult helyzetet befolyásolni.

Katonai természetű veszélyeztetésről akkor beszélhetünk, ha a válsághelyzet megoldására tett politikai, diplomáciai, gazdasági és egyéb lépések nem járnak eredménnyel, és a felek között a viszony tovább romlik. Ez katonai természetű nyomásgyakorlás, erődemonstráció, provokációk, csapatösszevonások és határsértések formájában nyilvánul meg.

A *konfliktus utáni békeállapot* jellemzője, hogy a béke fenntartása és megerősítése érdekében általában olyan intézkedéseket léptetnek érvénybe, amelyek megakadályozzák az esetleges konfrontációkat. A feszültségszintet csökkentő intézkedések elhúzódó alkalmazása azonban a végleges békeállapot létrejöttét késleltetheti. Michael S. Lund feltételezése alapján – főként a diplomáciai, a politikai, a nemzetközi szervezetek és a katonai erő lépéseit tekintve – egy konfliktus szakaszai diagramszerűen ábrázolhatók.



12. ábra: A válság szakaszai, intenzitása és az alkalmazott fegyverek típusai
Forrás: Resperger (2002): 151.

5.4. A válságkezelés új megközelítése

A korábbi, Lund-féle válsággörbe változásait nyomon követve készítettem el a válságtípusok és a válságok intenzitás szerinti besorolását.

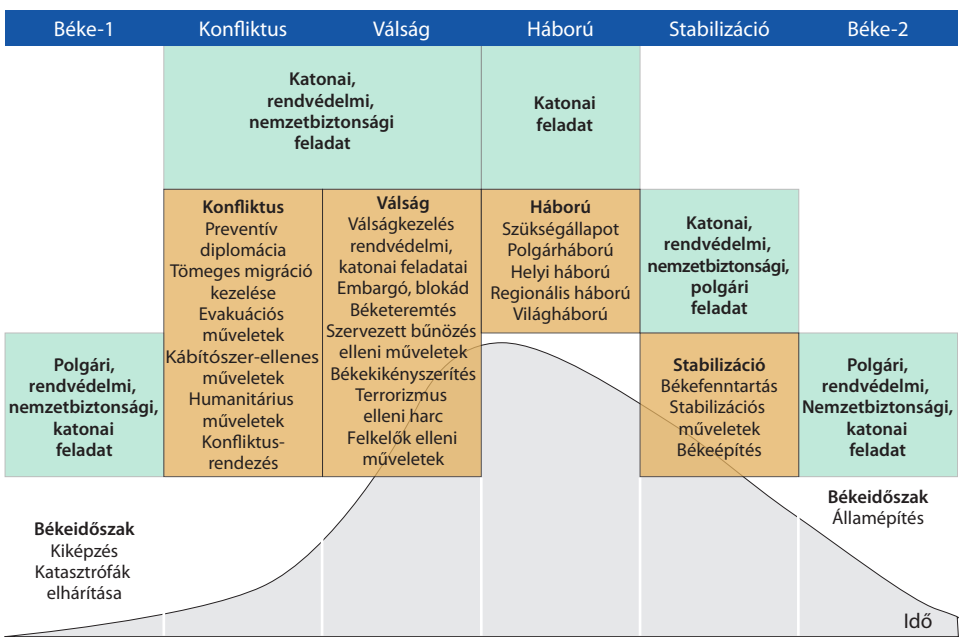
A *12. ábra* csak a békeműveleteket tartalmazza, de a jelenkor biztonsági környezete azt mutatja, hogy többféle válsággal kell szembenéznünk. A másik fontos érv a *12. ábra* további bővítése mellett, hogy az csak az állami szereplők figyelembevételével készült. A nem állami szereplők egyre nagyobb térnyerése – Iszlám Állam, felkelők, lázadók, szervezett bűnözők – azonban azt mutatja, hogy a konfliktusokban egyre többször legalább az egyik oldalon nem állami fél az aktor. A másik indok pedig, hogy megváltozott a válságok intenzitása, kiterjedése, így a kezelésük egyre bonyolultabbá, többszereplőssé vált. A korábbi „tiszta" katonai, belbiztonsági válságok helyébe az összetettebb, több állami és nem állami szereplőt igénylő kockázatok kerültek. A nemzetbiztonsági, a rendvédelmi, a katonai és a polgári szereplők a legtöbbször együtt dolgoznak a válságok kezelésén, elhárításán és a konfliktus utáni feladatok megoldásában. A legjobb példája ennek talán a napjainkban is zajló tömeges illegális migráció okozta veszélyhelyzet kezelése. Ebben a szituációban a kormányzati intézkedések alapján Magyarország ideiglenes biztonsági határzárat telepített a veszélyeztetett irányok, határszakaszok lezárására. A honvédelmi és a rendvédelmi tárca a nemzetbiztonsági szolgálatokkal, a nem állami szervezetekkel, a nemzetközi segélyszervezetekkel együttműködésben kezeli a térséget veszélyeztető problémát. Ha áttekintjük az állami szereplők előtt álló kihívásokat, a következő sokrétű feladatokat körvonalazhatjuk egy ilyen típusú válság kezelése során. A polgári és katonai nemzetbiztonsági

szolgálatok fő feladata információk szerzése a tömegeket kibocsátó országokról, a válságokról, a területről, a lakosságról; a migrációs útvonalak, nemzetközi embercsempész- és szervezett bűnözői körök felderítése. A rendvédelmi és katonai erők feladata a határ műszaki biztosítása, a műszaki zárak ellenőrzése, járőrözés, a Magyarország területére jogosulatlanul belépők feltartóztatása. A nemzetközi segélyszervezetek és a nem állami szervezetek pedig a migránsok ellátására és segítésére összpontosítanak.

A *13. ábra* a különböző típusú műveleteket (a migráció kezelésében történő részvétel, a kábítószer, a szervezett bűnözés és a terrorizmus elleni tevékenység) és a tipikus békeműveleteket tartalmazza (preventív diplomácia, béketeremtés, -kikényszerítés, -fenntartás, -építés). A konfliktus, a válság, a háború, a stabilizáció és a béke állapotához a megfelelő katonai, rendvédelmi, nemzetbiztonsági és polgári tevékenység tartozik.

– Az *első lépésben* a béke, célként a stabilitás jelenik meg, békeidőszakra jellemző kiképzéssel, fegyverhasználat nélkül.
– A *második rész,* a konfliktus időszaka tartalmazza a migráció és a kábítószer elleni tevékenységet.
– A *harmadik lépcsőfok* a válságkezelés rendvédelmi, nemzetbiztonsági és katonai feladatait valósítja meg.
– A *negyedik szakaszban* pedig az embargó, a blokád, a szervezett bűnözés elleni harc, a legmagasabb pontjaként pedig a béketeremtő akciók jelennek meg.

Ezen feladatok egyike sem csak a fegyveres erő tevékenységére jellemző, hiszen a sokoldalú válság sokoldalú megközelítést, sokszereplős tevékenységet igényel. A háború fázisa a legrövidebb, ugyanakkor a legnagyobb intenzitású szakasz, a bevetett erők, a fegyverek típusa szerint is.



13. ábra: A műveletek és intenzitásuk
Forrás: Resperger 2016a: 50.

A deeszkaláció időszakát a békefenntartás, a békeépítés, a stabilizációs műveletek és a tanácsadás, a kiképzés feladataival jellemezhetjük. Rendszerint ekkor történik a katonai erők kivonása, a feladatok átadása a rendvédelmi és a polgári szervezetek részére. A cél a béke stabilizálása, az államépítés feladatainak biztosítása. Ilyenkor a hagyományos rendészeti feladatok, a belrend, a közbiztonság megteremtése és fenntartása kerül előtérbe.

Az egyes műveletek nem csak egy fázisban, hanem minden időszakban jelen lehetnek. Ilyenek például a kábítósz-erellenes műveletek, a szervezett bűnözés elleni küzdelem vagy a migráció kezelése. Fontos megjegyezni továbbá, hogy a különböző típusú válságfajták hosszú időszakot ölelhetnek fel, illetve egyes típusok több időszakon keresztül is folyhatnak. Ilyenek a migráció kezelése, a kábítószer-ellenes műveletek, a szervezett bűnözők elleni küzdelem, a humanitárius műveletek, a blokád, az embargó vagy a terrorizmus elleni küzdelem.

5.5. A 21. század biztonsági kihívásai

5.5.1. A demográfiai robbanás és következményei

A globális kihívások közé tartozik a Föld népességének növekedése. Bolygónkat 2024-ben mintegy 8,161 milliárd ember lakta. 2050-re a népesség várhatóan 9,664 milliárdra nő, 2100-ra ez a szám már 10,18 milliárdra emelkedhet. A legnagyobb gondot Afrika és Dél-Ázsia igen gyors demográfiai növekedése, valamint Európa népességének csökkenése és elöregedése okozza. A demográfiailag gyorsan fejlődő országokat a *2. táblázat* mutatja be: újabb országok kerülnek demográfiailag fejlődő szakaszba, mint Irán, India és Brazília.

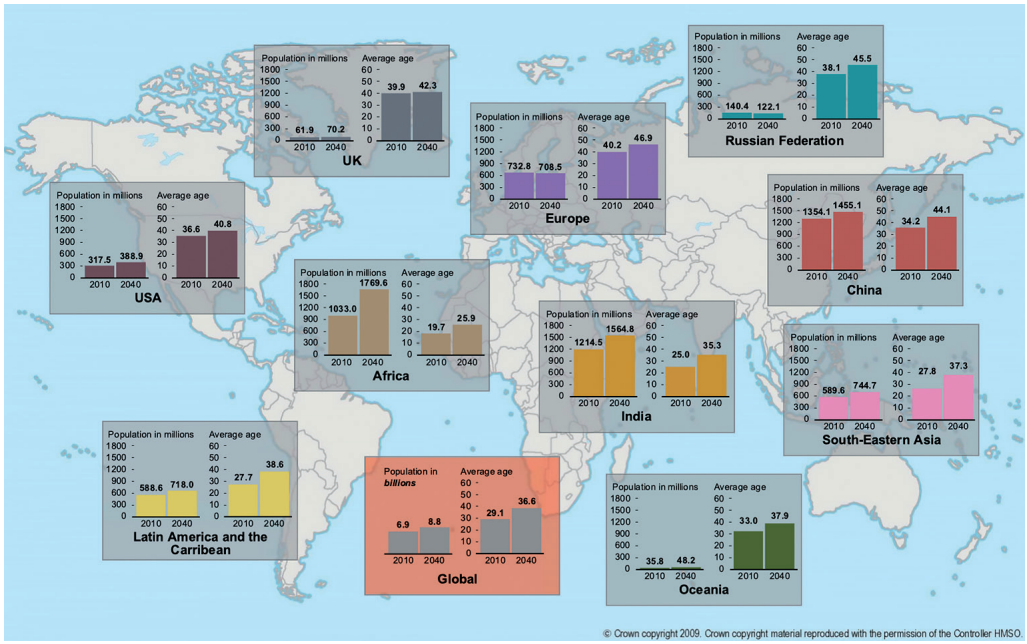
2. táblázat: A különböző országok demográfiai fejlődése

Ország	Átlagéletkor 2010-ben (év)	Átlagéletkor 2020-ban (év)	Átlagéletkor 2030-ban (év)	Demográfiai fejlődési szakasz
Brazília	29	33,2	35	2000–2030
India	26	28,7	32	2015–2050
Kína	35	38,4	43	1990–2025
Irán	26	31,7	37	2005–2040
Oroszország	39	40,3	44	1950–2015
USA	37	38,5	39	1970–2010

Forrás: Global Trends 2030: Alternative Worlds: 24.

A népességnövekedés az egyes földrészeket eltérő módon érinti. Az afrikai kontinens népessége 1950 óta 5,5-szörösére nőtt, Latin-Amerikáé és a Karib-szigeteké, valamint Ázsiáé és Óceániáé pedig több mint 3-szorosára. Észak-Amerika lakossága mindeközben a duplájára emelkedett. A legkisebb növekedés Európában következett be, mindössze 1,4-szeres gyarapodással.

Mindez átrajzolta a Föld népességének kontinensek közötti megoszlását. 1950-ben Ázsia lakossága tette ki a világ népességének 55%-át, ez 2017-ben 60%-ra (4,5 milliárdra) emelkedett. Afrika népességének részesedése ugyanezen időszak alatt 9-ről 17%-ra (1,3 milliárdra) nőtt. 2050-ben a fejlettebb világ lélekszáma várhatóan a 2000-es szint közelében alakul, a fejlődő országoknak viszont már legalább 7,8 milliárd lakosa lesz. (Tehát 1 : 6,5 arány prognosztizálható.)



14. ábra: A világ régióinak demográfiai változása, 2010–2040
Forrás: Strategic Trends Programme. Global Strategic Trends – Out to 2040. [é. n.].

Európa 1950-ben a Föld népességének még több mint egyötödét adta, napjainkban – 742 millió fővel – alig az egytizedét teszi ki. A világ két legnépesebb országában, Kínában és Indiában a Föld lakosságának 19%-a (1,4 milliárd fő), illetve 18%-a (1,3 milliárd fő) él. A két ázsiai országban külön-külön is többen élnek, mint a három legkisebb lakosságú kontinensen együttvéve. Az Eurostat adatai[1] szerint az unió 28 tagországának népessége 2016. január 1-jén 510,3 millió fő volt. A népességnövekedés 1960 óta töretlen – kivéve a 2019–2020-as Covid-időszakot –, és összességében az elmúlt több mint fél évszázadban közel 104 millió fővel, 20%-kal emelkedett az unióban élők száma. Az Eurostat által készített prognózis alapváltozata szerint az unió népessége a 21. század közepéig – lassú ütemben – folyamatosan növekedhet: 2045-ben elérheti maximumát, 529,1 millió főt. Ezt követően a trend lassú csökkenésbe, majd stagnálásba mehet át, 2080-ra az unió lakossága 518,8 millió főre mérséklődhet. 2080-ban az Eurostat számításai szerint 82,4 millió fős lakosságával az egykori és mai tagországok közül az Egyesült Királyság lehet a legnépesebb. 1800-ban például a Föld teljes népességének csak 3–5%-a volt városlakó, 2000-re ez már 47%-ra nőtt. Ma már az emberiség többsége városokban él. 2030-ra – egy ENSZ-előrejelzés szerint – közel 5 milliárd fő lesz városlakó, azaz az akkori teljes népesség legalább 60%-a.

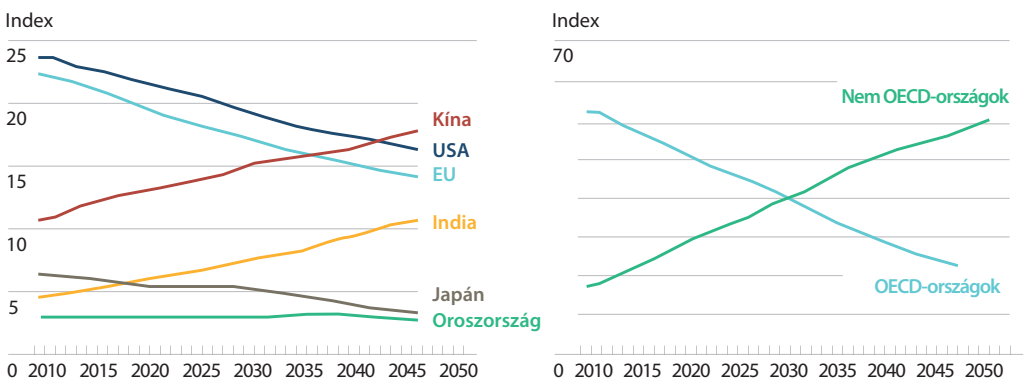
A vallási adatokat és arányokat tekintve a világ népessége a *3. táblázatban* vázoltak szerint oszlik meg, és arányaiban így változhat majd.

[1] Népességszerkezet és a népesség elöregedése. *Ec.europa.eu,* 2017. december 5. Online: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:N%C3%A9pess%C3%A9gszerkezet_%C3%A9s_a_n%C3%A9pess%C3%A9g_el%C3%B6reged%C3%A9se&oldid=365035

3. táblázat: A nagyobb vallási csoportok híveinek száma és százalékos aránya a Föld népességén belül

	2010	2050	2070	2100
Keresztények	2,16 milliárd fő 31,4%	2,92 milliárd fő 31,4%	3,96 milliárd fő 32,3%	3,78 milliárd fő 33,8%
Muszlimok	1,6 milliárd fő 23,2%	2,76 milliárd fő 29,7%	3,93 milliárd fő 32,3%	3,91 milliárd fő 34,9%
Vallás nélküliek	1,13 milliárd fő 16,4%	1,23 milliárd fő 13,2%	1,16 milliárd fő 10,5%	1,0 milliárd fő 9,0%
Hinduk	1,03 milliárd fő 15%	1,38 milliárd fő 14,9%	1,56 milliárd fő 14,1%	1,68 milliárd fő 15,2%
Buddhisták	487,76 millió fő 7,1%	486,27 millió fő 5,2%	423,3 millió fő 3,8%	224,2 millió fő 2,0%
Törzsi vallások	404,69 millió fő 5,9%	449,14 millió fő 4,8%	453,4 millió fő 4,1%	459,7 millió fő 4,2%
Zsidók	13,86 millió fő 0,2%	16,09 millió fő 0,2%	17,9 millió fő 0,15%	19,0 millió fő 0,17%
A világ népessége összesen	6,895 milliárd fő 100%	9,307 milliárd fő 100%	11,05 milliárd fő 100%	11,072 milliárd fő 100%

Forrás: The Future of World Religions: Population Growth Projections, 2010–2050



15. ábra: Az új, többkomponensű globális hatalom mutatói alapján számított hatalmi sorrend változásai 2050-ig
Forrás: Global Trends 2030: Alternative Worlds

A többkomponensű hatalom mutatói alapján (gazdasági, katonai, informatikai) 2030 lesz a váltópont a fejlett (OECD) és a fejlődő országok sorrendjében. 2030-tól az USA, Japán és Európa országai lefelé haladnak a listán, míg India, Kína és Oroszország felfelé indul.

A Magyarországra vonatkozó adatok szerint hazánk sajnos az elöregedő és fogyó nemzetekhez tartozik. Magyarország a 8,7 millióra becsült lélekszáma alapján megőrizheti a 13. helyét az európai rangsorban, miközben részaránya 1,9%-ról 1,7%-ra csökkenhet. Összességében a tíz évvel ezelőtti népszámlálások eredményeihez viszonyítva a Kárpát-medence lakosságszáma csökkent, és a csökkenés nagysága meghaladta az 1,1 milliót. A világ-, de főleg az európai trendet követve a demográfia dimenziójában, hasonlóan alakul Magyarország helyzete, hiszen az elöregedés, a fogyás lesz jellemző hosszú távon.

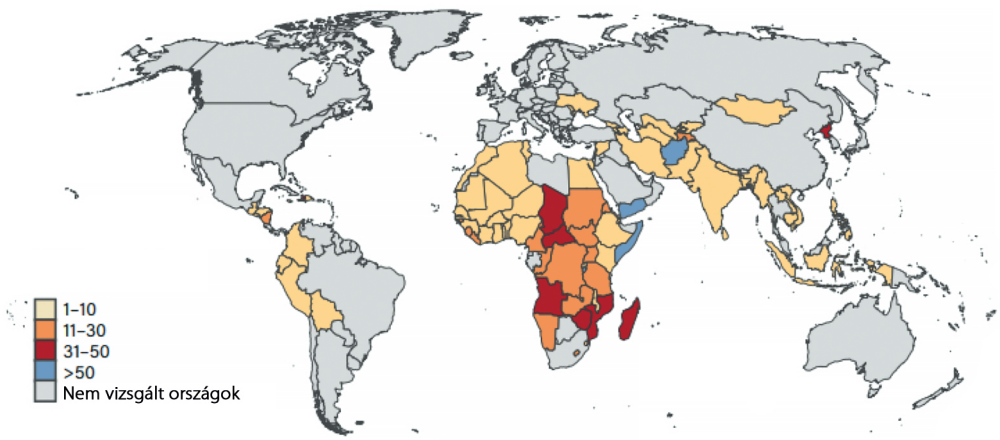
A lakosság létszámának alakulása a következő volt: 1900: 6,854; 1950: 9,293; 1989: 10,421; 2017: 9,798; 2024-ben 9,585 millió fő. 2025-ben 9,540 millió fő, 2030-ban 9,520 millió fő, 2050-ben 9,041 millió fő, 2100-ban 7,788 millió fő lesz. A jelenlegi migrációs trendek fennmaradását

feltételezve a lakosság száma 2020-ban 9,2 és 9,5 millió között, 2050-ben 7,5 és 8,7 millió között alakul majd. A 65 éven felüliek aránya 2020-ra elérte a 20,5%-os értéket. Az idős népesség eltartottsági jelzőszáma – amely az idősek számát a 15–64 évesek arányában fejezi ki – 24,6%, és ez az előrejelzések szerint 2050-re megkétszereződhet. Az ország öregedési indexe 126,1 – ez azt jelenti, hogy 100 fő 0–14 év közötti személyre 126 fő 65 éves és annál idősebb ember jut.

5.5.2. Az élelem, a víz, az ásványkincsek és az energiahordozók hiánya

5.5.2.1. Élelmiszerhiány

A demográfiai robbanás miatt a növekvő lakosság élelmezése egyre nagyobb gondot jelent. Az előrejelzések szerint 2030-ra 60%-kal nő a világ szükséglete élelmiszerből, takarmányból és rostanyagból *(16. ábra).* 2040-re a világ népességszáma valószínűleg 8,8 milliárd főre fog emelkedni, ami növekvő élelmiszer- és vízellátási igényt is jelent. Tekintettel arra, hogy a mezőgazdaság több mint 70%-át teszi ki a globális édesvízhasználatnak, az élelmiszer és a víz elérhetősége szorosan összefügg. Jelenleg a világban 886 millió fő alultáplált.



16. ábra: A várható élelmiszerhiány 2033-ban (%-ban)
Forrás: Food Security Assessment 2023–2033 [é. n.]

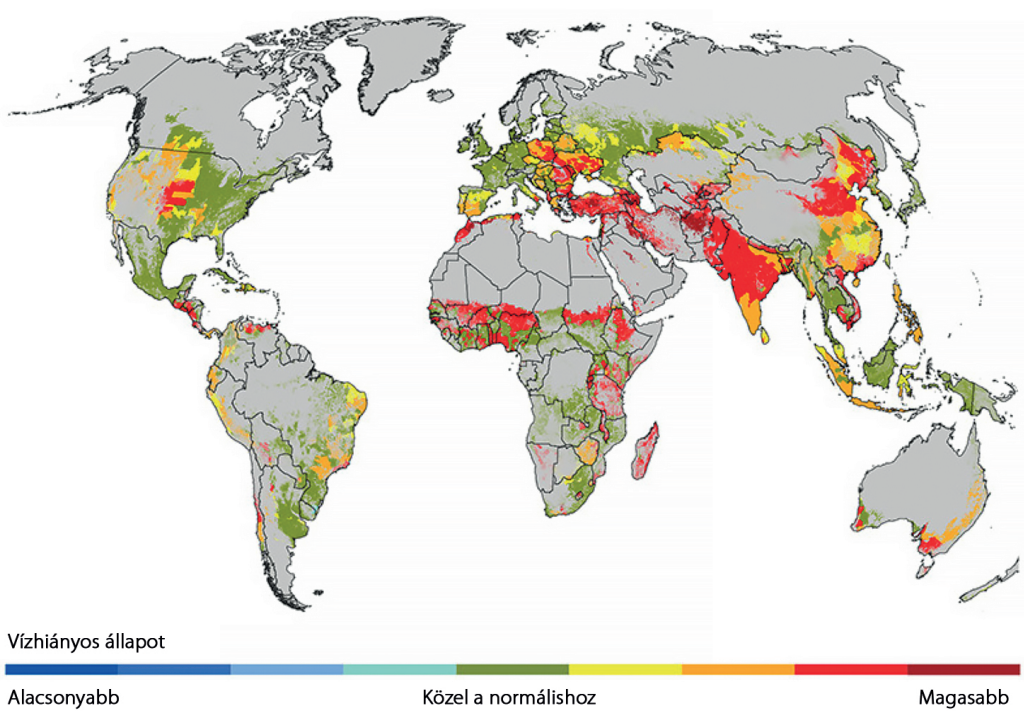
A Világbank szerint a világnak 50%-kal több élelmet kell termelnie, hogy 2050-ig az emberiséget táplálni tudja. Az éghajlatváltozás több mint 25%-kal csökkentheti a terméshozamot.

5.5.2.2. Vízhiány

Az élelmezés problémakörével szoros összefüggésben van az ivóvízkészlet feltárásának és elosztásának kérdésköre. Ahogy nő a Föld népessége, úgy nő az ivóvíz iránti igény. Sőt, a vízfelhasználás kétszer gyorsabb ütemben nőtt az elmúlt száz évben, mint a lakosság. A világ folyórendszereinek mára csaknem a fele károsodott valamilyen mértékben, és egyes folyók nem érik el az óceánt, kiszáradnak. Napjainkra a folyók csaknem 70%-ánál csökkent a vízhozam világszerte.

A folyók, tavak apadásának egyik oka az éghajlatváltozás, amely módosítja a csapadék eloszlását, fokozza a párolgást. Az ENSZ szerint 2040-re már 30%-kal nagyobb lesz az ivóvíz iránti kereslet, mint a kiaknázható készletek. Egyetlen kilogramm rizs előállításához legalább 5000 liter, a kávé esetében viszont már 22 ezer liter vízre van szükség. Bolygónk vízkészleteinek csak 2,5%-a az ember számára hasznos édesvíz. Ennek is a 69%-a gleccserekben és a sarkkörök állandó hó- és jégtakaróiban van, további 30%-ot pedig olyan föld alatti vízkészletek rejtenek, amelyekhez egyelőre vagy lehetetlenség hozzáférni, vagy kiaknázásuk túl energia- és költségigényes lenne.

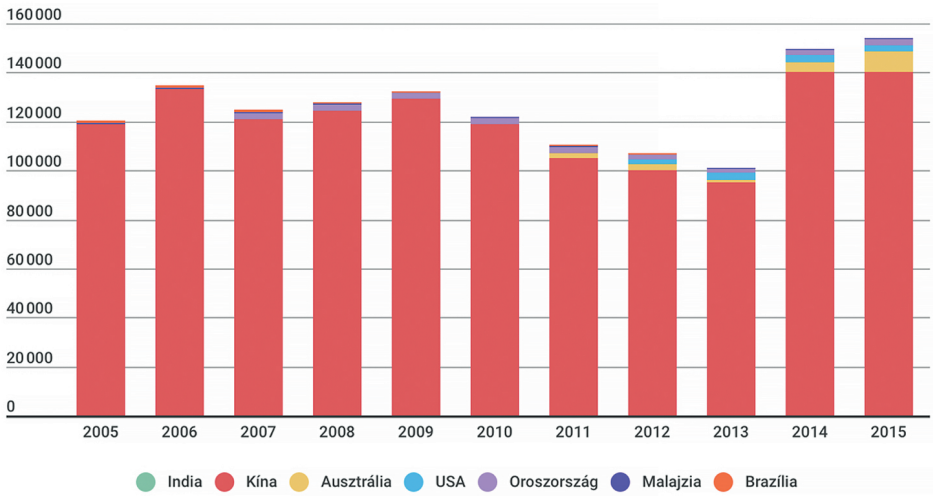
2025-ben 2,4–3,4 milliárd ember olyan országban fog élni, amely vízstresszes *(water-stressed),* azaz az 1 főre eső vízmennyiség nem éri el az 1700 köbmétert évente. Többnyire afrikai, közel-keleti, dél-ázsiai országokról és Észak-Kínáról van szó. Világszerte 200 főbb folyórendszeren osztozik két vagy több állam, ezek legtöbbje elosztási viták tárgyát képezi. Mind a felszíni, mind a föld alatti vízkészletek elosztásából származó konfliktusokra jó példákat szolgáltat a Közel-Kelet (a Jordán, a Nílus, a Tigris és az Eufrátesz). A becslések szerint körülbelül 2,5 milliárd ember él vízhiánytól sújtott régiókban, túlnyomórészt Afrikában, a Közel-Keleten, valamint Közép- és Kelet-Ázsiában. Csaknem 900 millió ember nem jut biztonságos ivóvízhez, ami több mint 5 millió halálesetet okoz évente *(17. ábra).*



17. ábra: A vízstresszes helyek a Földön (narancs, piros és bordó szín)
Forrás: Breene 2016

5.5.2.3. A kritikus fontosságú nyersanyagok

A jelenkor konfliktusai megmutatták, hogy a térségek egyenlőtlenül részesednek ezekből a polgári és katonai vállalatok számára fontos készletekből. Ebbe a körbe tartozik a lítium, mangán, antimon, berillium, gallium, germánium, grafit, indium, kobalt, króm, magnézium, molibdén, nikkel, platina, szilícium, tantál, wolfram *(18. ábra).*



18. ábra: A legnagyobb ritkaföldfém-bányász országok és termelésük (2007–2015, tonna)
Forrás: Tózsa 2025: 14.

19. ábra: A kritikus ritkafémek ellátásának veszélye a katonai eszközök gyártásánál
Forrás: Girardi et al. 2023: 5.

Jelenleg egyértelműen Kínától függ a ritka földfémekkel való ellátottság kérdése, a bányászat legjelentősebb részben Kínában történik, az elmúlt évtizedet tekintve toronymagasan vezet az ország, jóval 90%-ot meghaladó részesedéssel.

Az elemek egyértelműen szükségesek a modern rakéták, repülők, harcjárművek gyártásához.[2]

5.4.2.4. Növekvő nyersanyagigény

A Természetvédelmi Világalap *Élő bolygó* jelentése szerint a világnak 50%-kal több megújuló erőforrásra lenne szüksége, mint amennyit a Föld fenntartható módon nyújtani tud. Jelenleg évente 60 milliárd tonna erőforrást használnak fel világszerte – körülbelül 50%-kal többet, mint alig 30 évvel ezelőtt. 2000-ben egy Észak-Amerikában élő ember minden egyes nap 88 kg erőforrást használt el, míg Európában ez a szám napi 43 kg volt, Latin-Amerikában pedig napi 34 kg.

A világ számára szükséges stratégiai nyersanyagok eloszlása sem egységes. A szükséges stratégiai nyersanyagok – mint a kobalt, a króm, a platina, az antimon, az urán, a mangán és a volfrám – kitermelése és elosztása vitákat, konfliktusokat generálhat.

5.4.2.5. Az energiahordozók kimerülése

1981 és 2010 között a világ elsődleges energiafelhasználása 82%-kal nőtt, azaz az energiafogyasztás a 6,6 milliárd tonna kőolajnak megfelelő értékről 12 milliárd tonnára ugrott. 2011-ben 5,6%-kal bővült a globális energiafogyasztás – erre 1973 óta nem volt példa. 2030-ra az előrejelzések 16,5 milliárd tonnára becsülik az energiaigényt kőolaj-egyenértékben számolva, miközben a fogyó kőolajkészletek ellenére a 2020-as évek elején még közel 85–90%-os a fosszilis (nem megújuló) források aránya a világ energiafogyasztásában.

A gáz 69 évig, az olaj 79 évig – más források szerint 92 évig –, a barnakőszén 173 évig, a feketekőszén 102 évig áll az emberiség rendelkezésére. Ezek elfogyása után új energiahordozókra lesz szükség.

4. táblázat: Az USA és Oroszország kőolaj- és földgáztermelése és -tartalékai

Az USA és Oroszország kőolaj- és földgáztermelése				
	kőolaj		**földgáz**	
	súly	% a világ termeléséből	térfogat	% a világ termeléséből
USA termelése	827,1 millió tonna	18,3	1053,3 milliárd m^3	25,5
Oroszország termelése	541 millió tonna	12,0	586,4 milliárd m^3	14,4
Az USA kőolaj- és földgáztartalékai				
USA tartalékai	35,230 milliárd barrel	2,1	368,70 millió köbláb (1 köbláb – 28,316 liter)	5,3
Oroszország tartalékai	80 milliárd barrel	4,8	1688,2 millió köbláb (1 köbláb – 28,316 liter)	24,3

Forrás: BP Energy Outlook (2024) alapján a szerző szerkesztése

[2] Tózsa 2025.

A nukleáris energia rendszerbe állítása lassította az energiahordozók kiaknázásának ütemét, de számtalan újabb, megoldatlan kérdést vetett fel. A világ atomreaktorainak száma folyamatosan növekszik, napjainkban mintegy 440-re tehető. A hazánk területén található elsődleges (primer) energiahordozók az ország energiaigényének 50%-át adják. A nukleárisenergia-termelést is figyelembe véve a villamosenergia-függőségi mutatónk 60%. Az energiahordozók terén az importunk 2012–2013-ban 78,2%, 2021–2022-ben 93,3% volt földgáz tekintetében, az összes energiafüggőségünk 62,5%.

5.6. A világ kockázatai

5.6.1. Migrációs világtrendek, statisztikák

A világ több mint 7 milliárdos népessége gyarapszik és fiatalodik: 2050-re megközelíti a 9,8 milliárdot. A kialakult fejlettségi különbségek, konfliktusok és katasztrófák hatására a migráció több mint 150 millió embert érint világszerte. Habár a migráció volumene növekedett, a világ népességének csak kevesebb mint 3%-a élt egy évnél hosszabb ideig a hazáján kívül. A kutatások világszerte a migrációs nyomás erősödésére számítanak.

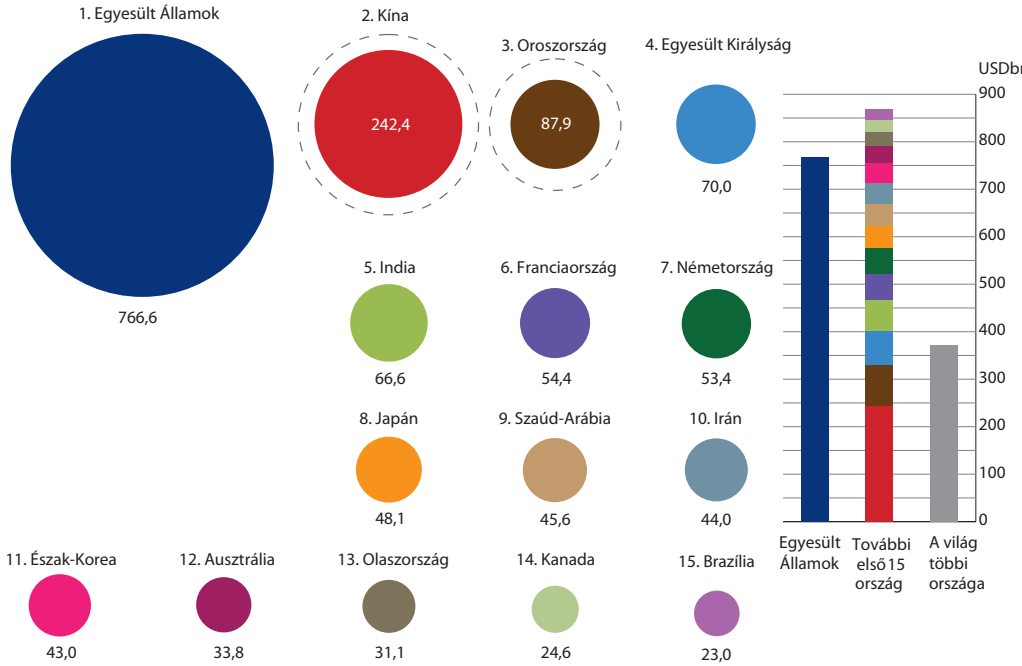
2025-re a menekültek száma elérte a 122,6 millió főt. Az ENSZ Menekültügyi Főbiztosságának (United Nations High Commissioner for Refugees, UNHCR) statisztikái szerint többségében üldözés, erőszak vagy az emberi jogok megsértése miatt voltak kénytelenek elhagyni a hazájukat. 2013-ban ez a szám még 8,3 millió fő volt, napjainkra eléri a 68,3 millió főt.

Az Európába irányuló fő migrációs útvonalak a szárazföldön: Törökország–Görögország–Macedónia, Szerbia–Magyarország/Horvátország. A tengeri útvonalak irányai: Nyugat-Afrika–Kanári-szigetek, Észak-Afrika–Szicília–Olaszország, Törökország–Görögország, Észak-Afrika–Spanyolország, Líbia–Olaszország, Egyiptom–Olaszország. Az európai közösség a tengeri útvonalak ellenőrzése, a migránsoknak való segítségnyújtás céljából több műveleti területen állomásoztat haditengerészeti erőket: Görögország, Olaszország, Gibraltár, Szardínia, Líbia.

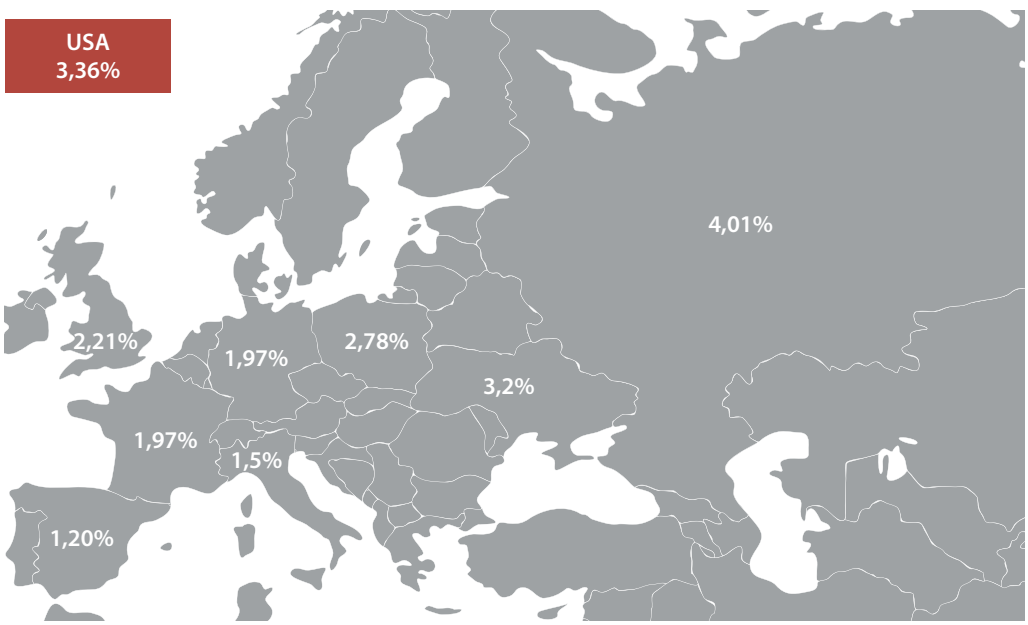
5.6.2. A fegyverkezésből és fegyverkereskedelemből fakadó problémák

A védelmi jellegű technológiák gyorsan fognak fejlődni a következő 15 évben, kiváltképp a nagy pontosságú fegyverek, az információs rendszerek és a kommunikáció, a drónok, a mesterséges intelligencia területén. Az orosz–ukrán háború, a közel-keleti konfliktus, az Izrael elleni terrortámadások felgyorsították ezeknek az új eszközöknek a tömeges alkalmazását (drónháború).

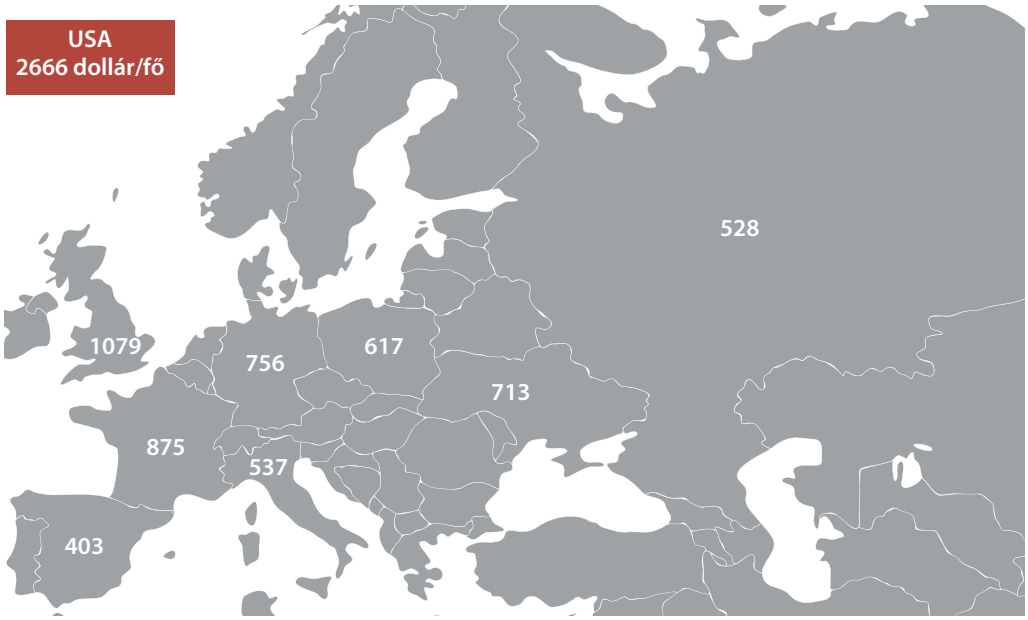
A fegyverek exportja akkor eredményezheti egy térség biztonsági stabilitásának felborulását, ha a meglévő katonai erőegyensúly megbontását idézi elő. A válságövezetekbe irányuló fegyverek gyakran fegyverkezési spirált indítanak el, ami a térségben a feszültség fokozódását, a katonai erő alkalmazásának lehetőségét vetíti előre. A védelmi kiadások mellett a GDP százalékos kiadásai és az egy főre jutó védelmi kiadások mutatják a legjobban az európai helyzetet *(20. ábra).*



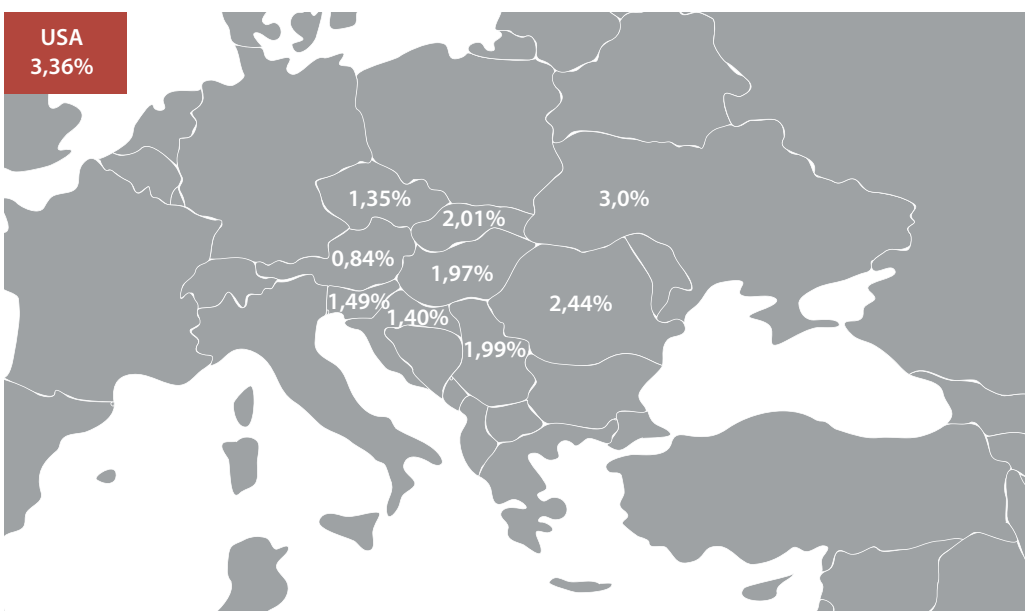
20. ábra: A 15 legnagyobb védelmi kiadással rendelkező ország (milliárd dollár)
Forrás: Military Balance 2024.



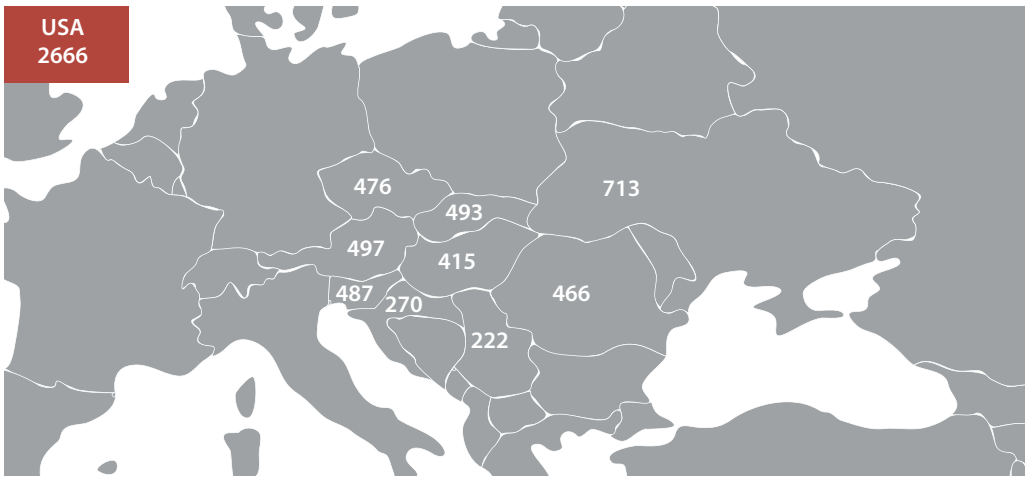
21. ábra: Védelmi kiadások a GDP százalékában (Nyugat- és Kelet-Európa)
Forrás: Military Balance 2023.



22. ábra: Egy főre eső védelmi kiadások dollárban (Nyugat- és Kelet-Európa)
Forrás: Military Balance 2023.



23. ábra: Védelmi kiadások a GDP százalékában (Közép-Európa és a Balkán)
Forrás: Military Balance 2023.



24. ábra: Egy főre eső védelmi kiadások USA-dollárban (Közép-Európa és a Balkán)
Forrás: Military Balance 2020.

5.6.3. A tömegpusztító fegyverek elterjedéséből adódó kockázatok

A nukleáris veszélyt növeli az a tény, hogy ötről (USA, Oroszország, Nagy-Britannia, Franciaország, Kína) kilencre nőtt az ilyen fegyverekkel rendelkező vagy azok előállítására képes és törekvő országok száma. A kis és közepes hatótávolságú ballisztikus rakéták, különösen ha tömegpusztító fegyvert hordoznak, már most is jelentősen fenyegetik az USA és a NATO-tagországok érdekeit, katonai erőit, illetve polgári lakosságát. Az Egyesült Államok és a világ többi része 2015 után fenyegetésekkel szembesült Észak-Korea részéről. Az atomfegyverek száma a világban: 12 121 darab.

A legnagyobb problémát az atomfegyver rendszeresítésére törekvő ország, országok jelenthetik (Irán). Ha a fegyverekkel terrorcsoportokat támogatnak, vagy fenyegetőznek a fegyverek bevetésével.

5. táblázat: Atomfegyverrel rendelkező országok listája

	Az első nukleáris teszt éve	Katonai raktárkészlet			Kivont eszközök	Összes készlet
		Stratégiai	Raktáron	Teljes		
USA	1945	1770	1930	3700	1477	**5328**
Oroszország	1949	1718	2591	4309	1150	**5580**
Nagy-Britannia	1952	120	105	225	–	**225**
Franciaország	1960	280	10	290	–	**290**
Kína	1964	24	576	600	–	**500**
India	1974	0	180	180	–	**172**
Pakisztán	1998	0	170	170	–	**170**
Izrael	–	0	90	90	–	**90**
Észak-Korea	2006	0	50	50	–	**50**
Összesen		**3912**	**5702**	**9614**	**2627**	**12 405**

Forrás: SIPRI (2025) alapján a szerző szerkesztése

5.7. A 21. század biztonsági fenyegetései

5.7.1. A terrorizmus

A világban 2023-ban a top 10 terrorszervezet összesen 1259 támadást követett el, a halálos áldozatok száma 3527, a sebesülteké 3224 volt.[3]

A globális adatok szerint a terrorizmus továbbra is jelentős kihívást jelent.

– Azon országok száma, ahol rögzítettek terrorista incidenst 2024-ben 58-ról 66 országra nőtt.
– A terrorizmus következtében elhunytak száma 7555-re csökkent 2024-ben, ami 13%-os csökkenés.

A legtöbb halálesetért felelős négy terrorista csoport 2024-ben az Iszlám Állam (IS), a Jama'a Nusrat ul-Islam wa al-Muslimin (JNIM), a Tehrik-e-Taliban Pakistan (TTP) és az al-Shabaab. 2007 óta a terrorizmus okozta halálesetek száma ingadozott, tetőzött 2015-ben 10 882 fő halálával, és 2022-ben elérte a 6 824-es mélypontot. Ebben az időszakban a terrorizmus dinamikája rendkívül változékony maradt, epicentruma a gyengébb országok felé tolódik el (2025).

Country	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2022	2024
Burkina Faso	114	113	111	110	52	30	21	15	7	6	4	2	1	1
Pakistan	2	2	2	2	4	4	5	5	5	8	9	7	4	2
Syria	19	4	4	5	6	7	7	8	6	5	6	5	5	3
Mali	40	22	19	21	16	13	10	9	8	7	7	4	3	4
Niger	50	60	45	34	19	19	18	19	14	12	8	10	10	5
Nigeria	8	5	5	3	2	2	4	4	4	4	5	8	8	6
Somalia	5	7	7	7	8	5	3	3	3	3	3	3	7	7
Israel	22	18	22	23	29	31	33	31	34	34	35	26	2	8
Afghanistan	3	3	3	4	3	3	2	2	1	1	1	1	6	9
Cameroon	49	57	58	19	11	11	12	10	10	11	12	11	12	10

25. ábra: A terrorizmussal legfőképpen érintett országok listája, 2011–2024 között
Forrás: Global Terrorism Index 2025

2001. szeptember 11-ével új időszámítás kezdődött a terrorizmus elleni küzdelemben. Az Amerikai Egyesült Államokban 1865. április 9-én véget ért a polgárháború, azóta amerikai földön nem érte ilyen súlyos veszteség az USA-t.

[3] Global Terrorism Index 2023: 14.

6. táblázat: A 2001. szeptember 11-ei terroresemények következményei

Mutatók	
A támadásokban elesett személyek száma	2819 fő
Megölt tűzoltók és mentők száma	343 fő
A rendőri tisztviselők és a kikötői hatósági rendőrök halottainak száma	60 fő
Az első toronyban elhunyt alkalmazottak száma	1402 fő
A második toronyban elhunyt alkalmazottak száma	614 fő
Embereket vesztett WTC-vállalatok száma	60 db
Azon nemzetek száma, amelyeknek polgárait megölték támadások során	115 db
A roncsok közül életben kimentett emberek	18 fő
Becsült véregység a New York-i vérközpontnak	36 000 adag
New York-i emberek száma, akik poszttraumás stressz-rendellenességben szenvednek a szeptember 11-i események eredményeként (becsült szám)	422 000 fő
A megsemmisült rendőri járművek száma	98 db
Az eltávolított törmelék mennyisége	**1 506 124 tonna**

Forrás: Statista 2012

A terrorista cselekmény következtében előtérbe került a terrorizmus, ezen belül a vallási indíttatású terrorizmus, valamint az ellene való küzdelem. Egy terrorista cselekmény fogalmának meghatározása során sokféle változattal találkozhatunk.

A terrorizmus: terroristák (egyének vagy csoportok) által, politikai célok elérése érdekében, főként a polgári lakosságon, erőszakos eszközökkel folytatott tevékenység abból a célból, hogy akaratukat az ellenfélre kényszerítsék.

A fogalmak közös jellemzőiként említhetjük:
- a politikai, vallási, ideológiai indíttatást;
- az erőszak alkalmazását;
- a félelem kiváltásának szándékát;
- a kormányzat és a társadalom megrendítését.

„Bizonyos tény, hogy nem minden muszlim terrorista, de ugyanolyan biztos és kivételesen fájdalmas, hogy szinte minden terrorista muszlim.” Abdul Rahman Al-Rased vallástudós szavai ezek, de nemcsak emiatt, hanem az elmúlt évek fanatikus, vallásilag motivált merényletei miatt külön is érdemes megvizsgálni a vallási (iszlám) indíttatású terrorizmust. A jelenkor egyik nagy fenyegetését a nemzetközi terroristahálózat, az Iszlám Állam jelenti. Habár a terrorizmus elleni küzdelemben sok sikert ért el a világ, meg kell állapítani: a hálózat még jelentős tartalékokkal rendelkezik.

Az Iszlám Állam igazi erejét a külföldi harcosok alkották. A dzsihádisták közel 80 országból érkeztek, létszámuk közel 20 ezer fő volt. A külföldi harcosok a következő országokból jöttek: Tunézia: 3000, Oroszország: 3000, Szaúd-Arábia: 2500, Marokkó: 1500, Jordánia: 1500, Franciaország: 1200, Törökország: 1000, Németország: 600 fő.

Az Iszlám Állam létszámának alakulása

– 2005: 1000 fő
– 2006: 1100 fő
– 2011: 1000–2000 fő
– 2014: 6–10 ezer fő
– 2014: 11 ezer fő (6000 fő Irakban, 3000–5000 fő Szíriában)
– 2015: 20–31,5 ezer fő

Az Iszlám Állam (IÁ) az al-Káida nemzetközi terrorszervezetből vált ki, az Abu Muszab az-Zarkávi vezette Jama'at al-Tawhid wal-Jihad nevű szervezethez tartozott, majd a térség vezető szervezetévé, sok más csoportosulás esernyőszervezetévé vált. Mint korábban az al-Káida, az Iszlám Állam is *primus inter pares* (első az egyenlők között) terroristaszervezetté vált, amelynek minden nagyobb terrorcsoport hűségesküt tett: a nigériai Boko Haram és a szomáliai al-Shabaab 2015 márciusában, a líbiai Iszlám Fiatalok Súra Tanácsa *(Islamic Youth Shura Council)* még 2014-ben, az afganisztáni tálibok 2015-ben.

Mit kínál az IÁ? Elsősorban az erőszak, a brutalitás kiélésének lehetőségét. Sikert és lehetőséget arra, hogy a sok vereséget, megaláztatást elszenvedett muszlim harcosok győztes szerepben jelenjenek meg, alakítsák a térség sorsát.

Az IÁ – nem egyszerű terrorszervezetként, hanem jól működő csoportként – hosszú távra is megtervezi tevékenységét. Tervezési módszereik és szintjeik között megtalálhatjuk a nagy stratégiai tervezést (politikai szint), a katonai stratégiai szint katonai céljait és a harcászati szintű módszereket, alkalmazásokat és eljárásokat is.

Az Iszlám Állam nagy stratégiája és katonai stratégiája

Az IÁ nagy stratégiája:
– a már az al-Káida által meghirdetett kalifátus létrehozása, az államhatárok lebontása a térségben;
– megalapítani és stabilizálni az Iszlám Államot;
– a muszlimok tömegeit idezarándokoltatni;
– a világban további terjeszkedés.

Az IÁ katonai stratégiája:
– a szunnita területek ellenőrzés alá vonása, a térség városainak és kritikus erőforrásainak ellenőrzése;
– védelmi zóna létrehozása a kurd területek határain a kurd katonai támadások ellen;
– a szíriai kormányerők és az iraki biztonsági erők további pusztítása, védelmi képességeik lebontása, felőrlése;
– az iraki területek elfoglalása, a síita területekről indítható támadások elleni védelem kialakítása;
– a szíriai területen az an-Núszra Front semlegesítése;
– további területek hódítása.

5.7.1.1. Az IÁ médiatevékenysége[4]

Korunkban a közösségi média, az internet minden kézbe, háztartásba elviszi azokat az üzeneteket, híreket, amelyeket a terrorszervezetek el kívánnak juttatni. Az IÁ tudatos, jól felépített információs, kommunikációs stratégiája többcélú volt:

- bemutatni a saját sikereiket;
- meggyőzni és befolyásolni a muszlim lakosságot;
- meggyőzni és befolyásolni más távolabbi muszlim országok lakosságát;
- a nyugati társadalmak felé hirdetni és terjeszteni az IÁ sikeres akcióit;
- a bemutatott események okán, a világ minden pontján csatlakozásra bírni a kisebb terrorszervezeteket, esetleges egyéni elkövetőket;
- olyan médiahatást elérni a világban, hogy folyamatos és szervezett toborzást lehessen folytatni a terrorszervezet javára.

Az elmúlt évek terrorista „főszereplője" az Iszlám Állam volt Szíriában és Irakban. A múltban alkalmazott erők, eszközök és eljárások nem tudták meggátolni a nemzetközi terrorizmus akcióit és az újabb akciók előkészítését. Tehát új, jobban felkészült erőkre, új és hatékonyabb eszközökre, új és sikeresebb harci eljárásokra van szükség a nemzetközi terrorizmus elleni küzdelemben. A háború fogalmának értelmezése egy régi klasszikus Carl von Clausewitz szerint:

„A háború tehát erőszak alkalmazása, hogy ellenfelünket akaratunk teljesítésére kényszerítsük."[5] Clausewitz fogalmának analógiájára az IÁ médiastratégája: terroristák (egyének vagy csoportok) által politikai, stratégiai, katonai és polgári célok elérése érdekében, minden médiafelületen (írott, elektronikus, közösségi média) azok minden eszközével folytatott stratégiai és napi kommunikációs tevékenység abból a célból, hogy a saját, a semleges és az ellenséges katonákat és polgárokat a saját akaratuknak megfelelően befolyásolják politikai, stratégiai műveleteik támogatása érdekében. A 2016-os EU-jelentés az Iszlám Állam többrétegű médiahálózatát a következőképpen osztja fel: a felső réteget Abu Bakr al-Bagdadi és szóvivője, Abu Muhammad al-Adnani képviselték, ők alkották meg a kommunikációs alapelveket, amelyeket az alsóbb rétegek dolgoznak fel.

26. ábra: Az Iszlám Állam kommunikációs struktúrája
Forrás: Resperger–Túri 2021: 136.

[4] Resperger–Túri 2021.
[5] Clausewitz 2014 [1832]: 37.

A második réteg a szervezet hivatalos médiumait tartalmazza, ilyen például az al-Hayat Médiaközpont, amelynek feladata a propaganda terjesztése különböző nyelveken. Ide tartozik még a *Dabiq* angol nyelvű lap és a francia *Dar al-Islam,* amelyek célja az európai lakosság toborzása. A harmadik réteg a kalifátusok alegységeinek propagandaüzeneteit tartalmazza, amelyek a működési területükről szóló jelentéseket és a végrehajtott feladataikat is bemutatják. Ezeket videó formájában teszik közzé azonos időben az alegységek. A negyedik réteget a szervezetet támogató csoportok alkothatják, azonban ezt az információt nem erősítette meg hivatalosan a terrorszervezet. Az ötödik réteget az Iszlám Állam által ellenőrzött területeken (vagy azokon kívül) megtalálható egyének és csoportok alkotják, akik a közösségimédia-fiókokon keresztül igyekeznek tanácsokkal ellátni a leendő újoncokat, azaz toboroznak *(26. ábra).*[6]

5.7.1.2. A veszteségek kérdése

Az Amerikai Egyesült Államok és szövetségesei a terrorizmus elleni küzdelemben is nagyon kritikusan tekintik a személyi veszteségeket. A fegyveres erőknek a lehető legkevesebb áldozattal kell a kitűzött célokat elérni. Az iraki háború tanulsága az, hogy a békeműveletekben más módszereket kellett volna alkalmazni az amerikai erőknek, vagy más csapatoknak átengedni a megszállt területeket. Ez nem következett be, így az amerikaiaknak több vesztesége van már, mint a háború folyamán. A harccselekmények alatt 382 halottat, 467 sebesültet és négy eltűnt személyt regisztráltak. Az eddigi veszteségek Irakban: 4586/4418 USA-halott, 31 994 USA-sebesült, Afganisztánban: 2452/2349 USA-halott, 20 149 USA-sebesült.[7] A hadműveletek időtartama alatt az RPG-7 kézi páncéltörő gránátvető támadása okozta a legtöbb veszteséget (32 halott/11,5%), a megszállás alatt a legtöbb problémát az öngyilkos bombamerényletek és a kézi légvédelmi rakéták okozták.[8]

7. táblázat: Az Egyesült Államok személyi veszteségei az eddigi háborúkban és bevetésekben

Háború	Időszak	Elesett	Sebesült
Első világháború	1917–1918	116 516	204 002
Második világháború	1941–1945	405 399	670 846
Koreai háború	1950–1953	36 574	103 284
Vietnámi háború	1964–1973	58 220	153 303
Kuvait felszabadítása	1991	382	467
Bevetési terület	**Időszak**	**Elesett**	**Sebesült**
Grenada	1983	19	119
Panama	1989	23	324
Szomália	1992–1994	43	153
Haiti	1994–1996	4	3
Afganisztán	2001–2021	2 349	20 149
Irak	**2003–2021**	**4 418**	**3 194**

Forrás: Defense Casualty Analysis System

[6] *European Union Terrorism Situation and Trend Report 2016* [é. n.]: 17.
[7] *Iraq News/Afghanistan News* [é. n.].
[8] Elliott 2003, vö: Coperdy 2003: 4.

8. táblázat: Az iraki hadszíntér halálos áldozatainak száma

	Hadsereg	Haditengerészet	Tengerészgyalogság	Légierő	Teljes
	2 536	64	852	29	3 481
Teljes	**3 237**	**107**	**1 023**	**51**	**4 418**

Forrás: Defense Casualty Analysis System

9. táblázat: Az iraki hadszíntér sebesültjeinek száma

	Hadsereg	Haditengerészet	Tengerészgyalogság	Légierő	Teljes
	22 248	671	8 625	450	31 994
Teljes	**22 248**	**671**	**8 625**	**450**	**31 994**

Forrás: Defense Casualty Analysis System

10. táblázat: Az afganisztáni hadszíntér halálos áldozatainak száma

	Hadsereg	Haditengerészet	Tengerészgyalogság	Légierő	Teljes
	1 328	85	378	54	1 845
Teljes	**1 662**	**127**	**460**	**100**	**2 349**

Forrás: Defense Casualty Analysis System

11. táblázat: Az afganisztáni hadszíntér sebesültjeinek száma

	Hadsereg	Haditengerészet	Tengerészgyalogság	Légierő	Teljes
	14 223	452	4 946	528	20 149
Teljes	**14 223**	**452**	**4 946**	**528**	**20 149**

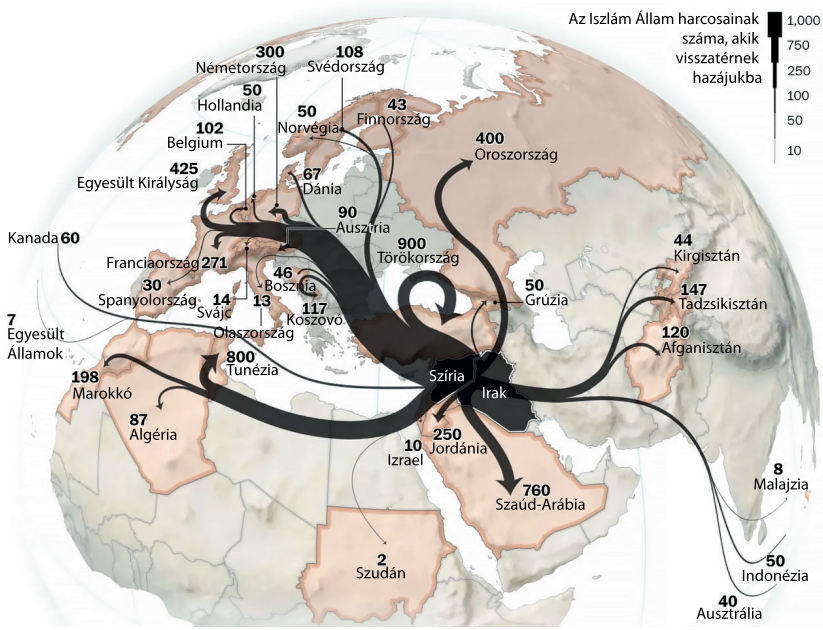
Forrás: Defense Casualty Analysis System

12. táblázat: Az Egyesült Államok személyi veszteségei a konfliktusokban, a halott–sebesült arány

Háború	Időszak	Elesett	Sebesült	Elesett–sebesült arány
Második világháború	1941–1945	405 399	670 846	1:1,65
Koreai háború	1950–1953	36 574	103 284	1:2,82
Vietnámi háború	1964–1973	58 220	153 303	1:2,63
Kuvait felszabadítása	1991	382	467	1:1,22
Afganisztán	2001–2021	2 349	20 149	**1:8,57**
Irak	2003–2021	4 418	31 994	**1:7,24**

Forrás: Defense Casualty Analysis System

A visszatérő harcosok száma a *27. ábra* szerint legmagasabb az Egyesült Királyságban és Németországban, Franciaországban, Szaúd-Arábiában, a Balkán országaiban, Algériában, Jordániában. A biztonságra nagy hatással lehetnek a visszatérők, ha nem megfelelő a nemzetbiztonsági szolgálatok tevékenysége, és nem alkalmazzák megfelelően ellenük a törvényeket.



27. ábra: Az Iszlám Állam terrorszervezetből visszatérő terroristák száma
Forrás: Meko 2018.

Sok esetben ezek az emberek megbánást mutatnak, kisebb szabálysértéseket és bűncselekményeket követnek el. De az ideológiájuk továbbra is veszélyes a demokratikus társadalmakra. Társadalmi szempontból a harcos példakép a muszlim kisebbségek számára, akit követhetnek, és egyenes út a radikalizációhoz. Az özvegyek kérdése is érdekes társadalmi feszültségeket, problémákat vetett fel. Ausztria, nem kívánta visszafogadni az IÁ özvegyeit, akik tőlük vándoroltak ki. Radikalizálódásukat, bosszúvágyukat erősnek érezték, mert az ENSZ menekülttáboraiban is felhúzták az IÁ zászlóját. Ideológiai beállítottságuk szélsőséges. A nyugati, demokratikus társadalomba való beilleszkedésük kérdéses. Az IÁ árvái tekintetében jobb volt a helyzet, több ország is százával fogadta be őket.

A békéhez mindenkinek a kompromisszumkészségét, erejét és akaratát kellene felmutatnia. Ahogy Napóleon fogalmazott: „A háborúhoz keménység, elszántság és állhatatosság szükséges." Úgy gondoljuk, ugyanezen képességekre lesz szükség a térség problémáinak rendezéséhez is.

5.7.2. A fegyveres konfliktusok, háborúk hatásai

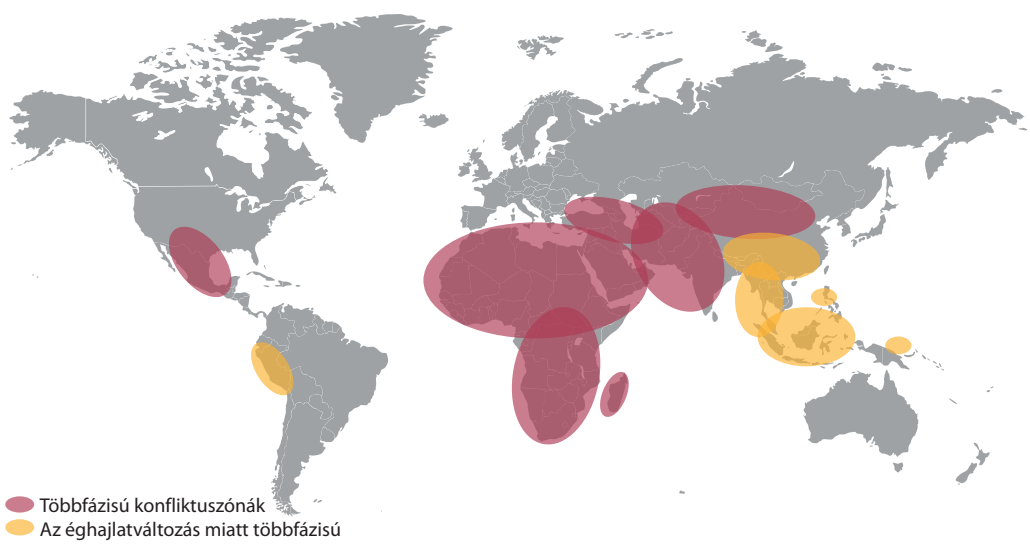
A két szuperhatalom szembenállásának időszakában is jelentős számú konfliktus, kihívás jelentkezett, de a hidegháború évei alatt ezek kevésbé voltak kiélezettek. 1945-től napjainkig a Földön csupán 26 nap telt el háború nélkül. A konfliktusokban, a konfliktusok mérete, intenzitása, az alkalmazott erők nagysága, a területi kiterjedése alapján az államok közötti harcokban 1998–2023 között 3 793 114 fő hunyt el. 2023-ban 42 darab egyoldalú (21 213 halott), 59 darab nem állami konfliktust (122 797 halott) és 75 darab államok közötti konfliktust (154 626 halott) regisztráltak. A legújabb adatok szerint a legbékésebb, legbiztonságosabb országok: Izland,

Dánia, Ausztria, Új-Zéland, Portugália, Csehország, Svájc, Kanada, Japán, Szlovénia, Finnország. A legkevésbé békés országok a következők: Szíria, Dél-Szudán, Irak, Afganisztán, Szomália, Jemen, Közép-afrikai Köztársaság, Ukrajna, Líbia, Szudán, Pakisztán. A 2024-es évben 122,6 millió menekültet regisztráltak az ENSZ szakosodott szervei. A fegyveres összeütközések hatásai közé sorolható még a gyerekkatonák részvétele is a harcokban, a környezeti károsodások – akár az öbölháborúban az olaj Arab-öbölbe (Perzsa-öbölbe) történő engedése és a kutak felgyújtása, akár Koszovóban a gyengített uránt tartalmazó lövedékek alkalmazása –, valamint a taposóaknák okozta károk és veszteségek.

A válságok mellett a stratégiai sokkok is nehezítik a béke és a biztonság megteremtését. Esetenként az egyszeri események olyan megszakításokat eredményezhetnek, amelyek befolyásolják a meglévő folyamatokat és átalakítják a stratégiai környezetet. Egy ilyen esemény stratégiai sokk. A nagy hatású, alacsony valószínűségű események történelmi példái a következők:

– a berlini fal ledöntése,
– a 2007–2008-as pénzügyi válság;
– a 2001. szeptember 11-i terrortámadások;
– a terrorszervezetek Izrael elleni támadása 2024-ben.

A stratégiai sokkok kaszkádhatásúak, és több, látszólag összefüggő és előre nem látható változáshoz vezetnek. Átformálják a stratégiai kontextust, megváltoztatják a viselkedést és a tevékenységet. A válság közép- és hosszú távú hatásai bizonytalanok, azonban ennek a stratégiai sokknak a hatásai mégis jelentősek vagy katasztrofálisak lehetnek. Magában foglalhatja a globalizációt is, amely társadalmi, gazdasági, pénzügyi és geopolitikai területeket rendezhet át. A 2040-ig terjedő időszakban a globális kölcsönös függés és a komplex rendszerekre való támaszkodás valószínűleg tovább fog nőni.



28. ábra: Többfázisú konfliktuszónák 2040-ben
Forrás: Strategic Trends Programme. Global Strategic Trends – Out to 2040. [é. n.].

Egy nagyon érdekes biztonsági helyzetet teremt a nagyhatalmak számára az északi- és a déli-sarki régió. Nemcsak a hajózási útvonalak kezelése, ellenőrzése szempontjából, hanem a térségekben található fosszilis energiahordozók és stratégiai ásványkincsek miatt is. A Jeges-tenger által a környező államok, különösen Oroszország és Kanada jelentős előnyt élvez majd az energiaforrásokhoz való hozzáférésben.

Az Antarktisz-szerződésrendszer, amely a 60. szélességi foktól délre eső területeket érinti, valószínűleg továbbra is fenntartja a környezetvédelmet és megakadályozza a terület katonai alkalmazását. Az Antarktisz területén nagy valószínűséggel a viták kizárhatók, de a déli térségben verseny alakulhat ki az energia és a halászati erőforrások tekintetében, a növekvő és feltörekvő hatalmak pedig kihasználhatják a helyzetet.

5.8. A jelenkori hadviselési módok összehasonlítása

5.8.1. Hagyományos hadviselés

A hagyományos műveletek aktorai az államok, amelyek viszonylagos erő- és eszközegyensúlyban vannak, stratégiai céljuk az ellenfél védtelenné tétele, akaratuk rákényszerítése, az ellenséges katonai erők megsemmisítése, területének elfoglalása, az ellenséges nép akaratának megtörése. Mindez főként katonai módszerek alkalmazásával történik, a stratégiai dimenziók közül az alapvető elem a katonai erő. Fő jellegzetesség a megsemmisítés. Az ilyen jellegű konfliktusok halott-sebesült aránya 1 : 3. A vezető szereplő a műveletek kezdetétől a befejezéséig az állam. Ilyen háború például az iraki–iráni háború vagy az USA vezette koalíció Irak ellen.

A háború fogalma:

„A háború tehát az erőszak alkalmazása, aminek célja, hogy az ellenfelet saját akaratunk teljesítésére kényszerítsük.” [9]

5.8.2. Aszimmetrikus hadviselés

A háború egyik különleges fajtája az aszimmetrikus hadviselés.

Aszimmetrikus hadviselés

Az aszimmetrikus hadviselés: pontosan körvonalazott politikai célok érdekében folytatott, gyakran több szervezet ideológiai, vallási, etnikai közösségén alapuló katonai és nem katonai műveleteket, eljárásokat és módszereket alkalmazó, közvetlen és közvetett hatásokra építő és egymás hatásait felerősítő, a biztonság különböző dimenzióinak területét veszélyeztető harcmodor, főként harcászati eljárás, amellyel rákényszeríthetjük akaratunkat az ellenségre. [10]

[9] Clausewitz 2014 [1832]: 39.
[10] Resperger–Kis–Somkúti 2013: 33.

Az aszimmetrikus műveletek alatt az államok nem állami szereplők elleni tevékenységét értjük. Stratégiai cél az ellenség kifárasztása, akaratunk rákényszerítése, az ellenség akaratának megtörése, kivéreztetése. Leggyakoribb a gerilla-, felkelő- és terroristamódszerek alkalmazása. Fő jellegzetesség a kifárasztás. A stratégiai dimenziók közül a fő elem az idő. Az ilyen jellegű konfliktusok halott-sebesült aránya 1 : 6–14. A vezető szereplő a műveletek kezdetétől a befejezéséig a fegyveres erők, a fegyveres csoportok. Ilyen az USA vezette koalíciónak az al-Káida terrorszervezet elleni tevékenysége.

Az aszimmetrikus konfliktusok egyik jellemzője, hogy a hadszíntér egy hatszög alakú sakktáblán játszódik. Az egyik szereplő az IÁ és támogatói, a kialakult koalíció és támogatói, a nemzetközi szervezetek (ENSZ, EBESZ, EU, Afrikai Unió), a nem állami szervezetek (NGO – Non Goverment Organisation).

A tábla közepén sajnos a belső menekültek és a lakosság található. A győzelmet az tudja kivívni, aki nemcsak a katonai győzelmet, hanem az azt követő békét is meg tudja nyerni, jobb állapotokat tud biztosítani a hosszú ideje szenvedő lakosságnak és a menekülteknek. Ebben a sok-sok szereplőt, aktív geopolitikai játékost (USA, Oroszország, Szaúd-Arábia, Törökország, Irán) és geopolitikai pillért (Szíria, Afganisztán, Irak) felvonultató történetben a sok nemzetiségi, vallási, etnikai ellentét sokkal élesebb formában befolyásolhatja a konfliktus kimenetelét.

Az Iszlám Állam tervezési módszereinek megismerésével levonhatjuk azt a következtetést, hogy egy tervszerűen, hatékonyan felépített és üzemeltetett, minden tervezési szintre (politikai stratégiai, katonai stratégia, harcászati módszerek) kiterjedő tevékenységgel álltunk szemben.

29. ábra: Az aszimmetrikus hadviselés színtere a hatszög alakú sakktábla
Forrás: a szerző szerkesztése

5.8.3. Hibrid hadviselés

Oroszország fegyveres konfliktusban folytatott módszerét a szakértők hibrid hadviselésnek nevezik.

Hibrid hadviselés

A hibrid hadviselés a hagyományos reguláris (lineáris, konvencionális) és az irreguláris (nem lineáris, nem konvencionális) hadviselés puha, közepes és kemény módszereinek, eljárásainak rugalmas alkalmazása abból a célból, hogy az ellenség államát, fegyveres erőit működésképtelenné, védtelenné tegyük és akaratunkat rákényszeríthessük, legfőképpen azzal a stratégiai céllal, hogy az erőszak szintje a konfliktus folyamán ne haladja meg a háborús szintet. [11]

A hibrid műveletek szereplői az államok és az irreguláris szervezetek az állam vagy államok ellen. A döntő erő- és eszközfölényben lévő fél alkalmazza. Stratégiai cél az ellenséges állam és a fegyveres erők működésképtelenné, védtelenné tétele, akaratunk rákényszerítése, az állam/nép akaratának a megtörése, az ellenséges állam/katonai erők működésképtelenné tétele, területének elfoglalása, elcsatolása. Fő módszer a reguláris/irreguláris katonai erők és a gerilla-, terroristaszervezetek, diplomáciai képviseletek, gazdasági módszerek felváltva történő alkalmazása. Fő jellegzetesség a kifárasztás és a működésképtelenné tétel. A stratégiai dimenziók közül a fő elem a katonai erő és az információ. Az ilyen jellegű konfliktusok halott-sebesült aránya 1 : 2,5–6. A vezető szereplő a műveletek kezdetétől a befejezéséig az állam. Ilyen például Oroszország háborúja Ukrajna ellen.

13. táblázat: A hadviselési módok összehasonlítása

	Hagyományos hadviselés	**Aszimmetrikus hadviselés**	**Hibrid hadviselés**
A hadviselés módja	reguláris erők összecsapása	– reguláris és irreguláris erők vagy – reguláris erők összecsapása	reguláris és irreguláris erők a reguláris és/vagy irreguláris erők ellen
Aktorok	állam(ok) – állam(ok)	– állam(ok) – nem állami szereplő, – állam(ok) – állam(ok)	állam(ok), nem állami szereplő(k) – állam(ok)
Alkalmazó fél	hasonló méretű haderők	– az egyik fél méretében, mennyiségében, módszereiben eltér, – általában a gyengébb fél alkalmazza	általában a túlerőben lévő fél alkalmazza
Stratégiai végállapot	az ellenfél védtelenné tétele, akaratunk rákényszerítése	– az ellenség kifárasztása, akaratunk rákényszerítése	az ellenséges állam és fegyveres erők működésképtelenné, védtelenné tétele, akaratunk rákényszerítése
Katonai végállapot (győzelem)	– az ellenséges katonai erők megsemmisítése, – a terület elfoglalása, – a nép akaratának a megtörése	– kifárasztás, – az ellenség akaratának megtörése, – kivéreztetés – a kivonulás elérése	– az állam/nép akaratának a megtörése, – az ellenséges állam/katonai erők működésképtelenné tétele, – a terület elfoglalása, elcsatolása

[11] Resperger 2018: 21.

	Hagyományos hadviselés	Aszimmetrikus hadviselés	Hibrid hadviselés
Módszer	katonai módszerek	gerilla-, felkelő-, terrorista-módszerek	– reguláris/irreguláris katonai, gerilla-, terrorista-módszerek – diplomáciai/gazdasági módszerek
A katonai és a polgári módszerek aránya	4 : 1	3 : 2	1 : 4
A fő hadviselési módszer	megsemmisítés	kifárasztás	– kifárasztás, – működésképtelenné tétel
A módszer jellege	egymást követő akciók	fokozatosan emelkedő intenzitás és erőszak	rugalmasan, felváltva alakított intenzitás és erőszak
A veszteségek aránya (halott-sebesült)	1 : 3	1 : 6–14	1 : 2,5–6
A fő stratégiai dimenzió	reguláris katonai erő	idő	– reguláris és irreguláris katonai erő, – információ, – diplomácia, – gazdaság, – média
A „clausewitzi állam, hadsereg, polgár hármas" vezetője a konfliktusban	állam	hadsereg	állam

Forrás: a szerző saját szerkesztése

Összefoglalva a három hadviselési módot megállapíthatjuk, hogy a hagyományos hadviselés katonai végállapotának hármas szabálya a hibrid műveletekre megfordult. A régi háborúkban jellemző „megsemmisíteni, elfoglalni, megtörni" elv helyébe az aszimmetrikus műveletekben a „kifárasztani, megtörni, kivéreztetni", a hibrid műveleteknél a „megtörni, működésképtelenné tenni, elfoglalni" elv lépett mint az elsőleges siker záloga. Az új típusú konfliktusok szereplőivel kapcsolatban a legfontosabb megállapítás az, hogy nincsenek érvényes szabályok – ez egyrészt az államiság hiányából, másrészt a felkelők, terroristák által követett stratégiából következik.

5.9. Magyarország biztonsági dimenzióinak értékelése

Hazánk biztonsági dimenzióinak értékelésénél fontos levonni a következtetést: a demográfiai mutatók alapján rövid (1–5 év), közép- (5–10 év) és hosszú távon (10–20 év) az ország érdekeire közepes és magas fenyegetést jelent hazánk elöregedése, a „fogyó nemzet" kategória. A migráció tekintetében közepes, a kábítószer elleni küzdelemben alacsony fenyegetettségként kell értékelnünk ezt a veszélyforrást. A terrorizmus – mint a fenyegetések legmagasabb szintje – középtávon nem, de hosszabb távon (közepes valószínűséggel) magas fenyegetést jelent társadalmunk számára.

14. táblázat: A transznacionális biztonsági dimenziók értékelése

Veszély-források	A kialakulás valószínűsége			Hatása az ország érdekeire		
	rövid távon	középtávon	hosszú távon	rövid távon	középtávon	hosszú távon
Demográfiai változások	alacsony	közepes	közepes	közepes	közepes	magas
Migrációs nyomás	közepes	közepes	közepes	közepes	közepes	közepes
Kábítószer-kereskedelem	alacsony	alacsony	alacsony	alacsony	alacsony	alacsony
Terrorizmus	alacsony	közepes	közepes	közepes	magas	magas
Energia-függőség	közepes	közepes	magas	közepes	közepes	magas

Forrás: a szerző szerkesztése

15. táblázat: A katonai, a kiber- és egyéb veszélyek értékelése

	A kialakulás valószínűsége			Hatása az ország érdekeire		
Katonai veszélyforrások	rövid távon	közép-távon	hosszú távon	rövid távon	közép-távon	hosszú távon
Nagy méretű fegyveres konfliktus	alacsony	közepes	közepes	magas	magas	magas
Regionális fegyveres konfliktus	alacsony	közepes	közepes	közepes	közepes	magas
Korlátozott célú, destabilizációs célú támadás	alacsony	alacsony	közepes	közepes	közepes	magas
Tömegpusztító fegyverek elterjedése	alacsony	közepes	közepes	közepes	közepes	magas
Katonai nyomásgyakorlás	alacsony	alacsony	közepes	közepes	közepes	magas
Extrémista fenyegetés	közepes	közepes	magas	magas	magas	magas
Kibertámadás	közepes	magas	magas	közepes	közepes	közepes
Szélsőséges társadalmi csoportok tevékenysége	alacsony	alacsony	közepes	alacsony	alacsony	közepes

Forrás: a szerző szerkesztése

A további területek megítélésénél a katonai dimenzióban nem számolhatunk közvetlen környezetünkben nagy fegyveres konfliktus bekövetkezésével. Közép- és hosszú távon a regionális fegyveres konfliktusok kialakulásának közepes valószínűsége is magas fenyegetést okozhat az ország érdekeinek érvényesítésében. A korlátozott célú destabilizációs agressziót középtávon nem zárhatjuk ki, illetve az ország értékeire és érdekeire gyakorolt fenyegetését magas szintre kell besorolnunk. A tömegpusztító fegyverek elterjedése akkor jelenthet reális fenyegetést, ha olyan országok kezébe kerül tömegpusztító fegyver és hordozóeszköz, amelyek a mi szövetségi rendszerünkkel (NATO, EU) ellentétbe kerülnek, és ezt nyomásgyakorlásként, reális elrettentő eszközként alkalmazhatják. A katonai nyomásgyakorlás bekövetkezhet, ha a környezetünkben lévő, nagy katonai potenciállal rendelkező ország valamilyen politikai, gazdasági vagy egyéb cél elérése érdekében hazánkra fegyveres, rendvédelmi vagy számítógépes hadviseléssel erőt alkalmaz, vagy azt kilátásba helyezi. Egy esetleges extrémista terrorista támadás főként hazánk nemzetközi szerepvállalása kapcsán fenyeget. Kibertámadás a világ bármely pontjáról indítható, az ország infrastruktúráját, vezetési, politikai, illetve bankrendszerét fenyegetheti már rövid

távon, magas károkozó képességgel. A szélsőséges társadalmi csoportok tevékenysége az ország demokratikus berendezkedését, államrendjét, a stabilitást, a jólétet fenyegetheti, hosszabb távon közepes nagyságú fenyegetéssel az érdekeinkre.

5.9.1. A kiberbiztonság alapvető feladatai

A digitalizáció rohamos fejlődése kihívások elé állítja nemcsak az egyéneket, de a szervezeteket is. Ahhoz, hogy a szervezet fennmaradjon, vagy el tudja látni a feladatait, jelentős informatikai támogatásra van szüksége, amelynek velejárója az információbiztonsági, kiberbiztonsági terület fejlesztése. A digitalizáció ugyanis nem csupán új eszközök és rendszerek bevezetését, üzemeltetését jelenti, hanem átfogó szemléletmódot, amely megköveteli a gyors reagálást és a naprakész, biztonságorientált gondolkodást. Ennek érdekében elengedhetetlenné válik a megfelelő védelmi stratégiák kialakítása és a tudatos, folyamatos innováció a szervezeti folyamatokban.

A feltörekvő felforgató technológiák – úgy, mint a mesterséges intelligencia, kvantum-számítástechnika, autonóm eszközök – gyökeresen alakítják át életünket. Az információs technológia által előállított értékek is egyre nagyobb hatással lesznek a szervezetek bevételeire, valamint az országok gazdaságára egyaránt. Az informatika oldaláról vizsgálva: az adatok mennyisége mellett a számítási kapacitás is növekszik, amelyet kezelni kell, ezáltal több szerepe lesz a jövőben például az *edge computingnak,* vagyis annak, hogy a számítási kapacitás – az adatok mozgatásával a hálózati forgalmat nem terhelve – átkerül az adatok keletkezésének helyszínéhez.

A kibertérből érkező fenyegetések tendenciái is alakulnak a technológiák fejlődésével, amit segít az is, hogy egyre könnyebben elérhető támadó, feltérképező szoftverek állnak a támadó oldal rendelkezésére. A támadáshoz már nem kell minden esetben szakértelem, mivel ezek az eszközök segítenek a technológia mély megértése nélkül is eredményt elérni esetenként. A kiberbűnözés mint szolgáltatás (CaaS[12]) modelljében a kiberbűnözők hacker- és más kiberbűnözési szolgáltatásokat nyújtanak, ami pénzért már bárki számára megvehető. Ezek közé tartoznak a felhőszolgáltatásként elérhető megoldások (például Ransomware as a Service [RaaS], Phishing as a Service [PhaaS] stb.), amelyek még jobban előtérbe helyezik az informatikai rendszerek védelmének szükségességét.

A kiberbiztonság – fogalom szerint – mint „azok a tevékenységek, amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és más személyeknek a védelméhez szükségesek”[13] jelentősége fokozatosan növekszik. Neves informatikai biztonsággal foglalkozó cégek és ügynökségek is évről évre megjelenítik a kiberbiztonsági jelentéseiket. Az ENISA *Threat Landscape 2024.* jelentésében a legnagyobb fenyegetések közé sorolja a következőket: zsarolóvírusok, kártékony kódok, *social engineering* fenyegetések, adatok elleni fenyegetések, rendelkezésre állás elleni fenyegetések (szolgáltatásmegtagadás és az internetes fenyegetések), információmanipuláció és zavarás, valamint ellátási láncot érintő támadások.[14]

[12] Cybercrime-as-a-Service (CaaS).

[13] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről.

[14] *ENISA Threat Landscape 2024* [é. n.].

A Microsoft 2024. évi digitális védelmi jelentése alapján a nemzetállami szereplők kiberműveletei is egyre globálisabbá váltak az elmúlt évben. A nemzetállamok felől érkező fenyegetések továbbra is egyre nagyobb méreteket öltenek és egyre kifinomultabbá válnak, a kormányok egyre inkább arra használják őket, hogy megértsék más nemzetek, transznacionális szervezetek terveit.[15]

A Verizon cég adatvédelmi incidensek kivizsgálásáról szóló jelentése szerint a jogsértések 68%-a hozható összefüggésbe az emberi tényezővel, ami magában foglalja a *social engineering* támadásokat, hibákat vagy visszaéléseket.[16] Az emberi tényezők között nagyon fontos megemlíteni a felsővezetői területet és annak elkötelezettségét, hozzáállását az IT-képességekhez. A felsővezetők gondolkodásának jelentős befolyása lehet az informatika területén dolgozó szakemberek sajátos világára, ezzel összefüggésben a kiberbiztonságra egyaránt. Bihari László és Magyar Sándor egy publikációban már olyan eseteket gyűjtött össze, amelyek az IT-terület negatív megítélését eredményezhetik, és megértésük tisztább képet tud adni, nemcsak az IT vagy IT biztonsági területen dolgozó szakembereknek, hanem a felettük, a mellettük lévő igénytámasztóknak egyaránt.[17]

5.9.2. Jogszabályi környezet

A korábbi 2013-as *Magyarország Nemzeti Kiberbiztonsági Stratégiája* jól felvázolta a kibertér definícióját, a terület komplexitását:

> „A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."

A definícióból egyből kitűnik, hogy nemcsak az informatika és a hozzá kapcsolódó technológiai területre kell fókuszálni kizárólag, hanem az emberi tényezőre, a szervezeti oldalra és az ahhoz kapcsolódó folyamatokra egyaránt. Sajnos sokszor előfordul, hogy az egyének mellett a szervezetek sem érzik komoly kockázatnak a kibertérből érkező fenyegetéseket. „Éppen ezért a jelenlegi technológiai környezetben – a már alkalmazott lokális katonai és nem katonai együttműködéseken, a jogi szabályozottságon túl – az egyének, valamint a felhasználói csoportok biztonságfelfogásában is jelentős változásokra lesz szükség." [18]

5.9.3. Magyarország Kiberbiztonsági Stratégiája

Magyarország kiberbiztonsági stratégiájának[19] (Stratégia) célja, hogy a digitális társadalom és infrastruktúra biztonságát megerősítse, tudatosságot építsen minden szinten (állampolgár – intézmény – állam)

[15] *Microsoft Digital Defense Report 2024* [é. n.].
[16] Verizon 2024.
[17] Bihari–Magyar 2020.
[18] Magyar–Simon 2017.
[19] 1089/2025. (III. 31.) Korm. határozat Magyarország Kiberbiztonsági Stratégiájáról.

és biztosítsa az EU- és a NATO-tagságból fakadó elvárások teljesítését, miközben elősegíti a kritikus információs infrastruktúrák ellenálló képességének növelését, támogatja a kiberbiztonsági innovációt és kutatás-fejlesztést, ösztönzi a köz- és magánszféra együttműködését, valamint hosszú távon fenntartható, adaptív és átlátható szabályozási és intézményi kereteket hoz létre a folyamatosan változó kibertér kihívásainak kezelésére.

A 2025-ös kiberbiztonsági stratégia átfogó megközelítést alkalmaz, amely túlmutat a pusztán technológiai vagy jogi aspektusokon, és a kiberbiztonságot társadalmi jelentőségű feladatként kezeli. A digitális állam gondolatának előtérbe kerülése, a piaci és a civil szféra aktív bevonása, valamint a kiberbiztonság közszolgáltatásként történő értelmezése új, hangsúlyos irányokat jelölt ki. A stratégia egy ágazatokon átívelő, horizontális kormányzási modellt követ, amely az együttműködésen és a közös felelősségvállaláson alapul. Ez a tematikus fejlődési irány jól illeszkedik a nemzetközi kiberbiztonsági trendekhez. Globálisan is megfigyelhető, hogy a kiberbiztonság egyre inkább multidiszciplináris és több szereplőt összefogó területté válik, ahol az állami, gazdasági és civil szektor közötti együttműködés elengedhetetlen a hatékony védelem megteremtéséhez.[20]

A honvédelmi ágazat oldaláról a Stratégia megjeleníti a kibervédelmi képességek fejlesztését, fenntartását és a honvédelmi gazdasági társaságok magas szintű kiberbiztonságának állami felügyeletét. Prioritásként kezeli a kritikus infrastruktúrák egységes védelmét, valamint az állami és gazdasági szereplők közötti kommunikáció és kríziskezelési együttműködés erősítését. Alapvető cél a személyi állomány folyamatos képzése, a tudatosság fejlesztése kibergyakorlatokkal, valamint a nemzetközi együttműködés fenntartása. Kiemelt fontosságú továbbá a kiberműveleti képességek fejlesztése, különösen a kognitív hadviselés elleni védelem érdekében.

5.9.4. Magyarország kiberbiztonsági törvénye a honvédelmi ágazat oldaláról megközelítve

Magyarország kiberbiztonsági törvénye[21] egy átfogó, az európai uniós szabályokkal összhangban álló rendszert vezet be, amely kötelezővé teszi a szervezetek számára a kockázatok azonosítását, kezelését és rendszereik biztonsági besorolását. A jogszabály erősíti a hatósági kontrollt, lehetőséget ad szankciók alkalmazására, és előírja a tanúsítási, valamint rendszeres ellenőrzési folyamatokat. Ennek eredményeként az ország jóval felkészültebbé válik a kibertámadásokkal és más digitális fenyegetésekkel szemben.

A honvédelmi célú informatikai rendszerek kiberbiztonságáért erre, kormányrendeletben kijelölt hatóság felelős. Ez a honvédelmi kiberbiztonsági hatóság hasonló feladatokat lát el, mint a nemzeti kiberbiztonsági hatóság, de bizonyos kivételekkel, valamint speciális szabályok szerint működik, figyelembe véve a honvédelmi érdekeket.

A hatóság nyilvántartja a fontosabb adatokat és rendszereket, felügyeli a honvédelmi kiberbiztonsági szabályok betartását, és jogosult arra is, hogy ha olyan adat kerül fel az internetre, amely veszélyezteti a honvédelmet, akkor azt ideiglenesen elérhetetlenné tegye. A sérülékenységvizsgálatokat csak a honvédelmi kiberbiztonsági incidenskezelő központ végezheti.

Ez a központ felel a honvédelmi célú elektronikus információs rendszerek biztonságáért a gyakorlatban is: figyeli a fenyegetéseket, kezeli az incidenseket, reagál a válsághelyzetekre,

[20] Magyar et al. 2025.

[21] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról.

segíti az ügyfelei tájékozódását és képzését, illetve Magyarországot képviseli a nemzetközi kiberbiztonsági együttműködésekben is. Ha egy honvédelmi szervezet kibertámadást vagy gyanús eseményt észlel, köteles azt jelenteni ennek a központnak, amely a szükséges adatokat továbbítja a nemzeti incidenskezelő központ felé is.

5.9.5. A PreDeCo elv

A kiberbiztonság területén végzett tevékenységek többféleképpen megközelíthetők, azonban az egyik legelterjedtebb szemlélet a megelőző, észlelő, korrigáló (PreDeCo) elv szerinti csoportosítás. Ez az elv általában három fő kategóriát jelöl ki, amelyek egymást kiegészítve, rendszerszinten gondoskodnak a szervezet információbiztonságáról.

Például a SOC tevékenységei nem korlátozódnak kizárólag az észlelő funkciókra, hiszen proaktív, megelőző jellegű feladatai is vannak – különösen a *threat hunting* és *threat intelligence* módszerek alkalmazásában. A korrigáló tevékenységek (például az eseménykezelés) szintén kapcsolódik a hatósági feladatokhoz, hiszen egy biztonsági incidens kivizsgálása során, azt követően gyakran szükség lehet jogi, ellenőrzési és szabályozási eljárásokra is. Továbbá, bár a képzés elsődlegesen a megelőző tevékenységek körébe tartozik, az eseménykezelés során feltárt hiányosságok (például a nem megfelelő *hardening* vagy emberi mulasztás) szintén rámutathatnak a továbbfejlesztendő oktatási igényekre.

A fejezet további részében röviden, megemlítés szintjén térünk ki ezekre a területekre, hogy átfogó képet nyújtsunk a kiberbiztonsági tevékenységek sokszínűségéről és egymást kiegészítő jellegéről. A cél egy átfogó megközelítés kialakítása, amely a PreDeCo elv mentén biztosítja a szervezet folyamatos védelmét, miközben reagál a gyorsan fejlődő technológiai környezet új kihívásaira.

5.9.6. Megelőző feladatok

Hatósági feladatok. A Honvédelmi Kiberbiztonsági Hatóság feladata, hogy felügyelje a honvédelmi célú informatikai rendszerek biztonságát. Ellenőrzi a biztonsági felelősök alkalmasságát, jóváhagyja a rendszerek biztonsági besorolását, nyilvántartásokat vezet, biztonsági előírásokat, ajánlásokat ad ki, és nemzetközi szabványok alkalmazását követelheti meg. Folyamatosan ellenőrzi a rendszereket, feltárt hiányosságok esetén intézkedéseket rendel el, és szükség esetén korlátozhatja vagy megtilthatja a rendszerek használatát, a külföldi vagy felhőalapú adatkezelés tekintetében. Incidens esetén hivatalból eljárást indít, tájékoztatja az érintett hatóságokat és gyakorlatokat szervezhet, továbbá azokban közreműködhet. Emellett részt vesz a kiberbiztonsági tudatosság fejlesztésében, javaslatokat tehet kritikus szervezetek kijelölésére, és szakhatósági feladatokat is elláthat.

A hatóság részletes nyilvántartást vezet többek között a szervezetek elektronikus információs rendszereiről is. Ez a nyilvántartás magában foglalja a rendszerek megnevezését, biztonsági osztályát, valamint a meghatározott fizikai, logikai és adminisztratív védelmi intézkedéseket.[22]

[22] 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról.

A hatósági feladatok ily módon nem csupán jogi keretet biztosítanak, hanem a kiberbiztonsági kultúra megerősítéséhez is jelentősen hozzájárulnak a nemzeti szintű szabályozásban.

Szoftverek biztonsági bevizsgálása. A szoftverek életciklusuk során számos potenciális hibát, sebezhetőséget hordozhatnak, amelyeket a lehető leghamarabb azonosítani és orvosolni kell. A biztonsági bevizsgálás keretében mérik a kódban rejlő kockázatokat és azt, hogy a szoftver mennyire áll ellen a különböző kibertámadási technikáknak. Statikus szoftverbiztonsági vizsgálat során a forráskód elemzése segítségével már a fejlesztés korai szakaszában feltárhatók azok a hibák, amelyek később komoly biztonsági rést jelenthetnek. Ezzel nemcsak költséghatékonyabban lehet megelőzni egy esetleges incidens bekövetkezését, de a minőségi szoftverfejlesztés alapjait is megteremti. Dinamikus szoftverbiztonsági vizsgálat alatt a szoftver futás közbeni ellenőrzését hajtják végre, amely során szimulált támadásokkal vagy automatizált tesztekkel próbálják meg azonosítani a gyengeségeket. Ez a módszer már a valós működés közben világít rá a hibákra, segítve így a gyakorlati biztonsági szempontok beépítését a további fejlesztésekbe.

A két módszer kombinációja teszi lehetővé a szoftver legteljesebb körű vizsgálatát, ami elengedhetetlen a biztonságos üzemeltetéshez. Emellett gyakran alkalmaznak olyan szoftverfejlesztési keretrendszereket (például DevSecOps), amelyek integrált módon, folyamatosan ellenőrzik és javítják a kódbeli hibákat.

Sérülékenységvizsgálat. Magyarország kiberbiztonságáról szóló törvénye részletesen szabályozza a sérülékenységvizsgálat végrehajtásának kereteit. A sérülékenységvizsgálat olyan sérülékenységmenedzsment-eszköz vagy módszer, amely során informatikai rendszerek, hardverek és szoftverek biztonsági szempontú átvizsgálása zajlik, az ellenőrzést automatizált eszközökkel és közvetlen, szakértő által végzett vizsgálatokkal hajtják végre.[23] A megelőzés területén belül a sérülékenységvizsgálatnak igen fontos szerepe van, mégpedig a lehetséges gyengeségek, sebezhetőségek feltárása területen. A szervezete számára a beazonosított támadási felületek lehetőséget adnak arra, hogy a védelmi intézkedéseket meg lehessen hozni, még mielőtt azokat a támadások során kihasználhatnák. A sérülékenységvizsgálatok fókusza, tárgya és a végrehajtás módja esetenként eltérő lehet.

A módszertan általánosságban két fő kategóriát különböztet meg. A belső sérülékenységvizsgálat során történik a hálózat belső oldaláról végzett teszt, feltételezve, hogy a támadó már rendelkezik valamiféle belépési joggal vagy fizikai hozzáféréssel a rendszerekhez. Ennek célja, hogy megakadályozzuk a belső fenyegetések (például nem megfelelően képzett vagy rosszindulatú alkalmazottak) kihasználását. A külső (távoli) sérülékenység vizsgálatnál az internet felől érkező támadásokat modellezik, így ellenőrizve azt, hogy milyen kockázatokkal kell számolni a nyilvánosan elérhető rendszerek és szolgáltatások esetében. A sérülékenységvizsgálat rendszeres elvégzése, például havonta vagy negyedévente, vagy nagyobb rendszerfrissítések alkalmával kifejezetten ajánlott a kiberbiztonsági incidensek megelőzésének érdekében.

Behatolásvizsgálat. A behatolásvizsgálat során a cél annak azonosítása, hogy egy valódi támadó mit tudna tenni az informatikai rendszerben található sebezhetőségekkel. Itt etikus hackelési tevékenység során meggyőződnek a rendszer megfelelő beállításairól, a szoftverkomponensek frissítettségéről, gyenge, sebezhető pontjairól. Ezen proaktív tevékenység során kézi és automatikus vizsgálatot végezhetnek a szakemberek. Ugyanúgy, mint a sérülékenységvizsgálat során, itt is a sebezhetőségek keresése a cél, de itt a rendszerbe történő behatolás megtörténik, és tesztelik, ellenőrzik azt, hogy a talált sérülékenységek valóban mennyire használhatók ki.

[23] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról, 89. pont.

A *hardening* során a szervezet informatikai rendszereinek megerősítése kerül a középpontba, mivel a használhatóság és a rendelkezésre állás mellett ma már a biztonság az egyik legfontosabb szempont. A védelem felépítése sokrétű, magában foglalja többek között az alábbiakat:

- jelszavak erősítése: komplex, megfelelő hosszúságú és rendszeresen frissített jelszavak alkalmazása;
- fiókkezelés és jogosultságok: a felesleges vagy inaktív felhasználói fiókok törlése, a jogosultságok minimálisra szorítása (legkisebb jogosultság elve – *least privilege*);
- felesleges szolgáltatások letiltása: csak a valóban szükséges protokollok, portok és funkciók maradjanak aktívak;
- titkosítás és naplózás: a rendszeres naplózás, monitorozás és a titkosított adatátvitel alapkövetelmény;
- a rendszeres frissítések és biztonsági javítások telepítése megelőzi az ismert sebezhetőségek kihasználását, így egy átfogó *patch-menedzsment* jelentősen növeli a szervezet biztonsági ellenálló képességét.

A mobileszközök elterjedésével a *mobile device management* (MDM) és hasonló megoldások kiemelt figyelmet kapnak, hogy a hordozható eszközök is a szervezeti *hardening* szabályoknak megfelelően legyenek konfigurálva a teljes életciklusuk során. Ez magában foglalja a biztonságos beállításokat, a rendszeres frissítéseket, valamint az időben történő selejtezést és adatmegsemmisítést is.

A kiberbiztonság területén alapvető megelőző intézkedés a rendszerek, hálózatok és adatok elkülönítése, azaz a szegregációja. Ennek lényege, hogy egy adott rendszer, illetve szolgáltatás kompromittálása ne terjedhessen át könnyedén a szervezet teljes infrastruktúrájára. A fizikai szeparáció – például külön szerverhelyiségek kialakítása vagy elkülönített eszközpark alkalmazása – mellett egyre inkább előtérbe kerül a logikai alapú, hálózati szegmentálás. A megfelelően kialakított elkülönítési stratégiák jelentősen korlátozhatják a kártékony tevékenységek mozgásterét, és megkönnyítik a biztonsági incidensekre adott gyors és célzott reagálást. Mindez hozzájárul a szervezet folyamatos működésének védelméhez és a kockázatok hatékonyabb kezeléséhez.

Tudatosítás. A feltörekvő, felforgató technológiák ugrásszerűen fejlődnek (például: mesterséges intelligencia, kvantum-számítástechnika stb.). Ezzel párhuzamosan a támadási technikák, mint például a *social engineering* technikák is javulnak, nagyobb intenzitásúvá válnak. A nyílt forrású információszerzés (OSINT) lehetőségei az internet penetrációjával egyre jobban megnövekedtek. Ezzel együtt az álhírek terjedése és hatásai emelkedtek.

Amennyiben az üzleti folyamatok vannak kizárólag szem előtt tartva, és nem jut elég erőforrás a védelmi intézkedésekre, a kibertámadások sikeressége nagyobb lesz a szervezetnél.

> „A menedzsment módszertanok a biztonsági kultúra eredményes megvalósítását lehetővé tevő sikertényezők között első helyen tartalmazzák a felsővezetés elkötelezettségét. Sőt, több módszertan odáig megy, hogy azt mondja, ennek hiányában nekikezdeni sem érdemes, mert eleve kudarcra van ítélve a kezdeményezés."[24]

A vezetői elkötelezettség nélkül – amely a feltételeket biztosíthatja – a SOC csak a nevében jelenthet biztonságot.[25]

[24] Horváth 2013.
[25] Schinagl–Schoon–Paans 2015.

Képzés. Fontos, hogy mindenki – a rendszergazdától a hétköznapi irodai dolgozóig – tisztában legyen az alapvető kiberbiztonsági elvekkel. A technikai tudás mellett ma már az is fontos, hogy az emberek felismerjék a gyanús jeleket, tudják, mit tegyenek egy furcsa e-mail esetén, vagy hogyan jelenthetnek egy biztonsági eseményt.

Az informatikusoktól pedig még többet vár el a környezet, mivel nemcsak a rendszerek működéséért felelősek, hanem azok biztonságáért is. Ehhez elengedhetetlen a folyamatos tanulás, hiszen a támadási módszerek is napról napra változnak. Egy jó informatikus ma már nemcsak technikailag felkészült, hanem képes átlátni a teljes kockázati helyzetet, és megfelelően reagálni és dokumentálni is azt.

5.9.7. Észlelő tevékenység

Biztonsági műveleti központok. A SOC egy központosított kiberszervezeti elem, amelynek feladata a kibertérből érkező fenyegetések valós idejű észlelése és az azokra történő reagálás az események megelőzése, kezelése érdekében. Az informatikai hálózatok és rendszerek naplóadatainak folyamatos monitorozásával a támadások észlelése a szervezetek esetében már alapvető biztonsági funkció. A SOC három fő forrásból származó információval dolgozik: a naplóadatok, a hálózati forgalom, valamint a végpontvédelmek (AV,[26] EPP,[27] EDR[28]). A SOC természetesen a támadások elemzésével azonosítja azok jellemzőit, vagyis azt, hogy a támadás mikor, hogyan történt, és miért volt sikeres. Valós időben gyűjti és elemzi a naplóadatokat, a hálózati forgalmat és a végpontvédelmi rendszerek (például antivírus, EPP, EDR) riasztásait, központosítja a kockázatok észlelését és az incidensek kezelését, proaktív módon gyűjt és elemez fenyegetésinformációkat *(threat intelligence)*, *threat hunting* tevékenységet folytat, amely során célzottan és szisztematikusan keresi a rejtőzködő támadókat vagy ismeretlen, új fenyegetéseket.

A SOC-nak, érettségétől függően, a betudás (attribúció) és a proaktív fenyegetésvadászat *(threat hunting)* területén is fontos szerepe van.

A SOC érettségét több tényező is befolyásolja, például a rendelkezésre álló erőforrások, az alkalmazott eszközök kifinomultsága, a monitorozás automatizáltsága, illetve a szakembergárda képzettsége és tapasztalata. Egy magasabb érettségi szinttel rendelkező SOC képes nem csupán reagálni, hanem előre is jelezni bizonyos támadási mintákat, elősegítve a stratégiai szintű döntéshozatalt.

5.9.8. Elhárító feladatok

A kibertámadások egyre kifinomultabbá és gyakoribbá válásával egy időben az incidenskezelési stratégia kidolgozása is előtérbe kerül. Az incidenskezelés segítségével a szervezetek felkészülhetnek a gyors reagálásra, minimalizálhatják a potenciális károkat, továbbá tanulhatnak a korábbi eseményekből. A megfelelő incidenskezelési gyakorlatok nemcsak a technikai biztonságot erősítik, hanem a jogi megfelelést is biztosítják, valamint hozzájárulnak a szervezet hírnevének és ügyfélbizalmának megőrzéséhez.

[26] AV: *antivirus* – vírusirtó.

[27] EPP: *endpoint protection platforms* – végpontvédelmi platformok.

[28] EDR: *endpoint detection and response* – végponti észlelés és reagálás.

Incidens után a helyreállítás *(recovery)* és a normál működés visszaállítása kritikus. Ehhez rendszeres biztonsági mentések és jól dokumentált folyamatok szükségesek.

A digitális nyomozás során a szakemberek elemzik a logfájlokat, a rosszindulatú kódot, és rekonstruálják a támadók lépéseit. Ez feltárja a behatolás módját, a kihasznált sebezhetőségeket és a kár mértékét. Az eredmények segítenek a jövőbeli védekezésben és esetleges jogi eljárásokban is.

Az incidenskezelés jogi-szabályozási követelményeket is maga után von. A GDPR vagy HIPAA előírhatja az incidensek jelentését és az érintettek tájékoztatását. A nem megfelelő eljárás súlyos bírságokhoz vezethet, ezért a jogi szempontokat már a kezdetektől be kell építeni az incidenskezelési folyamatba. Az incidensek utólagos elemzése biztosítja a folyamatos fejlődést.

Már nem kérdéses az, hogy a szervezetek és az egyének elszenvednek-e kibertámadásokat a jövőben, a kérdés inkább az, hogy mekkora lesz a kár értéke. A kibertérből érkező fenyegetések számának és komplexitásának növekedése indokolja a többszintű védelmi intézkedések előtérbe helyezését. A technológia rohamos fejlődése megköveteli a védelmi terület folyamatos fejlesztését, amelyet ugyancsak átfogó megközelítéssel kell biztosítani. A kiberbiztonság területén az ellenálló képesség növelése a versenyképesség, az alaprendeltetés ellátása, a reputáció megóvása érdekében nélkülözhetetlen.

A kibertámadások elleni védekezés leghatékonyabb formája a proaktív védelem, vagyis a megelőzés. Számos védelmi intézkedés megelőzési formát említettünk, de a SOC és az abban dolgozó emberek jelentik az utolsó védelmi vonalat, akik felelősek a támadások sikeres felderítéséért és enyhítéséért vagy elhárításáért. Ebből kifolyólag a megelőzés több területe mellett a biztonsági műveleti központok nyújtotta észlelési tevékenység jelentősen hozzájárulhat a károk eszkalálódásának megfékezéséhez.[29]

A hatékony incidenskezelés az elkülönítés, a helyreállítás, a frissítések, a digitális nyomozás, a jogi megfelelés és a tapasztalatok kiértékelésének összehangolt működtetésén alapul, ami gyors és hatékony reagálást tesz lehetővé a kiberfenyegetésekre, valamint hozzájárul a szervezet hírnevének és ügyfélbizalmának megőrzéséhez.

Ajánlott irodalom

Boda József (2014): A nemzetközi szervezetek válságkezelő tevékenysége. *Nemzetbiztonsági Szemle,* 2(1), 43–62. Online: https://epa.oszk.hu/02500/02538/00002/pdf/EPA02538_nemzetbiztonsagi_szemle_2014_01_042-062.pdf

Kaiser Ferenc (2011): A túlnépesedés és globális biztonsági kihívásai. *Nemzet és Biztonság,* 4(8), 27–36. Online: https://folyoirat.ludovika.hu/index.php/neb/article/view/4872

Kőszegvári Tibor (1993–1996): A *közép-európai térség és Magyarország biztonságát fenyegető veszélyek az 1990-es években.* Budapest: Országos Kiemelésű Társadalomtudományi Kutatások.

Resperger István (2018): *Válságkezelés és hibrid hadviselés.* Budapest: Dialóg Campus.

Resperger István szerk. (2014): *Nemzetbiztonsági alapismeretek.* Budapest: Dialóg Campus.

[29] Vielberth et al. 2020.

Felhasznált források

1089/2025. Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

A World Perspective on Food Shortages. *Financial Times,* 2017. február 21. Online: www.ft.com/content/9d2b0b36-f784-11e6-9516-2d969e0d3b65

Bányász Péter et al. (2022): A videókonferencia-alkalmazások biztonsági kockázatai. *Acta Humana: Hungarian Centre for Human Rights Publications,* 10(4), 19–34. Online: https://doi.org/10.32566/ah.2022.4.2

Girardi, Benderta – Patrahau, Irina – Cisco, Giovanni – Rademaker, Michael: *Strategic Raw Materials for Defence. Mapping European Industry Needs.* The Hague Center for Strategic Studies, 2023. január. Online: https://hcss.nl/wp-content/uploads/2023/01/Strategic-Raw-Materials-for-Defence-HCSS-2023-V2.pdf

Bihari László – Magyar Sándor (2020): Mennyország helyett a pokolba, avagy az informatikai támogatás kihívásai. *Szakmai Szemle,* (4), 158–169. Online: www.researchgate.net/publication/372648912_Mennyorszag_helyett_a_pokolba_avagy_az_informatikai_tamogatas_kihivasai

Borzadva figyelnek a szakértők: Ezt a filmet már láttuk. *Vasárnapi Hírek,* 2014. július 6. Online: www.vasarnapihirek.hu/friss/ezt_a_filmet_mar_lattuk

BP Energy Outlook (2024). Online: www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/energy-outlook/bp-energy-outlook-2024.pdf

BP Statistical Review Of World Energy (2022). Online: www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2019-full-report.pdf

Breene, Keith (2016): Food Security and Why It Matters. *World Economic Forum,* 2016. január 18. Online: www.weforum.org/stories/2016/01/food-security-and-why-it-matters/

Challenges. *IEEE Access,* 8, 227756–227779. Online: https://doi.org/10.1109/ACCESS.2020.3045514

Clausewitz, Carl von (2014) [1832]: *A háborúról.* Budapest: Zrínyi.

Coperdy, George (2003): A Pivotal War. *Defense and Foreign Affairs Strategic Policy,* 4.

Defense Casualty Analysis System. Online: https://dcas.dmdc.osd.mil/dcas/pages/report_oif_all.xhtml

Elliott, Michael (2003): Lessons from the Rubble. *Time,* 2003. szeptember 01. Online: http://content.time.com/time/subscriber/article/0,33009,1005561-6,00.html

ENISA Threat Landscape 2024 [é. n.]. Online: www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

European Union Terrorism Situation and Trend Report 2016 [é. n.]. Online: www.europol.europa.eu/publications-events/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016

Food Security Assessment 2023–2033. Online: www.qassurance.com/food-security-assessment-2023-2033/

Föld Napja Alapítvány [é. n.]: *Túlhasználat.* Online: http://fna.hu/vilagfigyelo/tulhasznalat

Global Peace Index 2024. Online: www.economicsandpeace.org/wp-content/uploads/2024/06/GPI-2024-web.pdf

Global Terrorism Index 2022. Online: https://reliefweb.int/attachments/a62d4dc4-c69b-49ee-8ef5-50d98205e70d/GTI-2022-web_110522-1.pdf

Global Terrorism Index 2025. Online: https://reliefweb.int/report/world/global-terrorism-index-2025

Global Trends 2030. Alternative Worlds. National Intelligence Council. Online: https://info.publicintelligence.net/GlobalTrends2030.pdf

Hasim, Ahmed S. (2015): *From Al Kaida affiliate to the rise of the Islamic Caliphate: The evolution of the Islamic State of Iraq and Syria (ISIS).* RSiS: Nanyang Technological University.

Horváth Gergely Krisztián (2013): *Közérthetően (nem csak) az IT biztonságról.* Budapest: KIFÜ. Online: https://kifu.gov.hu/wp-content/uploads/2022/03/IT_brosura_v7.pdf

HORVÁTH Levente (2020): A kínai geopolitikai gondolkodásmód és az „Egy övezet, egy út" kezdeményezés. *Geopolitikai Szemle,* 2(4), 203–220. Online: https://vikek.eu/wp-content/uploads/2020/07/Geopolitikai-Szemle-No42020.1.sz%C3%A1m.pdf

Iraq News/Afghanistan News [é. n.]. Online: http://icasualties.org/

Központi Statisztikai Hivatal [é. n.]: *A világ népessége kontinensek szerint, 1950–2100.* Online: www.ksh.hu/interaktiv/grafikonok/vilag_nepessege.html

Központi Statisztikai Hivatal [é. n.]: *Népesség, népmozgalom (1900–).* Online: www.ksh.hu/docs/hun/xstadat/xstadat_hosszu/h_wdsd001a.html

Lewis, Jessica D. (2014): *The Islamic State. A counter-strategy for a counter-state.* Washington DC: Institute for the Study of War. Online: www.understandingwar.org/sites/default/files/Lewis-Center%20of%20gravity.pdf

Lund, Michael S. (1996): *Preventing violent conflicts. Strategy for preventive diplomacy.* Washington DC: United Stated Institute of Peace Press.

Magyar Sándor – Simon László (2017): A terrorizmus és indirekt hadviselése az EU kiberterében. *Szakmai Szemle,* 15(4), 57–68. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2017_4_szam.pdf

Magyar Sándor et al. (2025): Magyarország kibervédelmi stratégiáinak összehasonlítása és fejlődési íve 2013 és 2025 között. *Szakmai Szemle,* 23(1), 127–144. Online: www.researchgate.net/publication/394304867_Magyarorszag_kibervedelmi_strategiainak_osszehasonlitasa_es_fejlodesi_ive_2013_es_2025_kozott

Meko, Tim (2018): Now that the Islamic State has fallen in Iraq and Syria, where are all its fighters going? *The Washington Post,* 2018. február 22. Online: https://cdradical.hypotheses.org/files/2018/03/ISIS-fighters-returning-home-Washington-Post-201803.pdf

Microsoft Digital Defense Report 2024 [é. n.]. Online: www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Müller, Claudio – Rosta Gábor (2013): A legújabb szupervírusok. *Chip,* (5), 24–29.

Padányi József (2010): Az éghajlatváltozás hatásai és a katonai erő. In Kohut László et al.: *Az éghajlatváltozás hatása a biztonságra és a katonai erő alkalmazására.* Budapest: Stratégiai és Védelmi Kutatóintézet. 32–46.

Resperger István (2016a): A válságkezelés új megközelítése. *Hadtudományi Szemle,* 9(3), 30–56. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/7116/16_3_hm_resperger.pdf?sequence=2&isAllowed=y

Resperger István (2016b): „Nomen est omen" nevében a végzet(e)? – A hibrid fenyegetésekre adható válaszok, a kontrahibrid műveletek. *Terror és Elhárítás,* 5(1), 78–81.

Resperger István – Túri Viktória (2021): *Iszlám Állam modus operandi harctéren, médiában és a pszichológiában.* Budapest: KNBSZ. Online: https://bit.ly/4rJDjBh

Resperger István – Kis Álmos Péter – Somkúti Bálint (2013): *Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.* Budapest: Zrínyi.

Ruzsbaczky Zoltán (2015): Nem kér az iszlámból a britek többsége. *Magyar Nemzet,* 2015. április 12. Online: http://mno.hu/kulfold/nem-ker-az-iszlambol-a-britek-tobbsege-1280069

Schinagl, S – Schoon, KC – Paans, R (2015): A Framework for Designing a Security Operations Centre (SOC). In *Secure Cyberspace in 21st Century. Proceedings of the Hawaii International Conference*

on System Sciences (HICSS), 2015. január 8. Online: https://doi.ieeecomputersociety.org/10.1109/HICSS.2015.270

SIPRI (2017): Global Nuclear Weapons: Modernization Remains the Priority. *Sipri.org,* 2017. július 3. Online: www.sipri.org/media/press-release/2017/global-nuclear-weapons-modernization-remains-priority

SIPRI (2024): Role of Nuclear Weapons Grows as Geopolitical Relations Deteriorate – New SIPRI Yearbook Out Now. *Sipri.org,* 2024. június 3. Online: www.sipri.org/media/press-release/2024/role-nuclear-weapons-grows-geopolitical-relations-deteriorate-new-sipri-yearbook-out-now

SIPRI (2025): Nuclear Risks Grow as New Arms Race Looms – New SIPRI Yearbook Out Now. *Sipri.org,* 2025. június 17. Online: www.sipri.org/media/press-release/2025/nuclear-risks-grow-new-arms-race-looms-new-sipri-yearbook-out-now

Statista (2012): *Key figures on the Attacks on the World Trade Center in New York City Committed on September 11, 2001.* Online: www.statista.com/statistics/281075/key-figures-on-the-september-11-attacks/

Strategic Trends Programme. Global Strategic Trends – Out to 2040. [é. n.]. Online: www.stat.berkeley.edu/~aldous/Real-World/gst4_update9_Feb10.pdf

Strategic Trends Programme. Global Strategic Trends – Out to 2045. [é. n.]. Online: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/MinofDef_Global%20Strategic%20Trends%20-%202045.pdf

The Future of World Religions. Population Growth Projections, 2010–2050. [é. n.]. Online: www.pewforum.org/2015/04/02/religious-projections-2010-2050/

The Military Balance 2025. Online: www.iiss.org/publications/the-military-balance

Tózsa István szerk. (2025): *Fémek a gazdaságtörténetben és a geopolitikában.* Kecskemét: Neumann János Egyetem. Online: https://geo.nje.hu/storage/content/4441/files/01_Femek.pdf?r=95269eff2d68dd189f426e40fd158b8c

United Nations (2013): *The Six Grave Violations Against Children During Armed Conflict: The Legal Foundation.* Working Paper Nº 1. New York. Online: https://childrenandarmedconflict.un.org/publications/WorkingPaper-1_SixGraveViolationsLegalFoundation.pdf

Verizon (2024): *Data Breach Investigations Report (DBIR).* Online: www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf

Vielberth, Manfred et al. (2020): Security Operations Center: A Systematic Study and Open

Ellenőrző kérdések

1. Hogyan alakul a világ demográfiai fejlődése az elkövetkező 20–30 évben?
2. Milyen tendenciák érvényesülnek a tömegpusztító fegyverek kapcsán?
3. Milyen tendenciát követ a világ fegyverkezése?
4. Jellemezze a hagyományos hadviselést!
5. Határozza meg az aszimmetrikus hadviselés jellemzőit!
6. Mi jellemzi a hibrid típusú hadviselést?
7. Ismertesse az Iszlám Állam terrorszervezet jellemzőit