Hadtudományi Szemle
18. évfolyam (2025) 4. szám 139–153. • DOI: 10.32563/HSZ.2025.4.9

Seprényi Patrik[1]

Az új technológiák problematikájának megjelenése a NATO biztonságfelfogásában

The Emergence of New Technologies as a Security Issue in NATO's Security Conception

Absztrakt

Napjainkban a globális hatalmi verseny egyik legfontosabb szegmense a technológiai előny megszerzése és/vagy megtartása elsősorban annak érdekében, hogy a nemzetközi tér adott szereplője biztosítani tudja a saját oldal külső fenyegetésekkel szembeni védelmét. A gyors ütemű technológiai fejlődés, különösen a korszakalkotó technológiák (Emerging and Disruptive Technologies, EDT) alapjaiban formálják át a nemzetközi biztonsági környezetet, és ezen technológiák gyors adaptálása és alkalmazásba vétele kellő elrettentő erővel bírhat az ellenfelek agresszív cselekedeteinek prevenciójához. Ennek megfelelően a NATO is igyekszik a technológiai fölény megtartására, hogy a jövőben is képes legyen ellátni egyik alapvető feladatát, az elrettentés és a védelem biztosítását. A tanulmány célja megvizsgálni, hogy a technológiai verseny hogyan alakítja a NATO biztonságfelfogását, illetve hogyan adaptálja vagy tervezi adaptálni a szövetség az új technológiai vívmányokat.

Kulcsszavak: technológiai fejlődés, technológiai verseny, korszakalkotó technológiák, NATO DIANA, adaptáció, mesterséges intelligencia (MI)

Abstract

Nowadays, one of the most important segments of global power competition is gaining and/or maintaining technological advantage, primarily so that a given actor in the international arena can ensure its own protection against external threats.

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola.

Rapid technological development, especially in the field of Emerging and Disruptive Technologies (EDT), is fundamentally reshaping the international security environment, and the rapid adaptation and deployment of these technologies can serve as a sufficient deterrent to prevent aggressive actions by adversaries. Accordingly, NATO is also striving to maintain its technological superiority so that it can continue to fulfil one of its fundamental tasks, namely deterrence and defence, in the future. The aim of this study is to examine how technological competition shapes NATO's approach to security and how the Alliance adapts or plans to adapt to new technological advances.

Keywords: technological development, technological competition, emerging and disruptive technologies, NATO DIANA, adaptation, artificial intelligence

Bevezetés

A történelem során az ellenségénél jobb fegyverek, fejlettebb technológiák előállítására való törekvés mindig is kulcsfontosságú szerepet töltött be a hadviselő vagy hadviselésre készülő felek tervezési folyamataiban. A jobb technológia sokszor a győzelem kulcsa lehet, így például hatalmas jelentősége volt a II. világháborúban a nyugati szövetségesek fejlett radartechnológiájának, valamint tengeralattjáró-elhárító sündisznóbombáinak *(hedgehog anti-submarine weapon),* amelyek révén hatalmas veszteségek keletkeztek a német tengeralattjárók soraiban.[2] Az atombomba születése pedig máig is érvényes hatású, hiszen a nukleáris képességek az elrettentő erő alapját képezik.[3]

A haditechnika, harceszközök, katonai technológia fejlődésének ívét hosszan lehetne részletezni a múltba visszatekintve, viszont azért, hogy minél hamarabb jelenkorunk kihívásait mutathassam be, mindössze egyetlen markáns fejlődési aspektust emelnék ki. Az emberiség a hőlégballonos megfigyeléstől kevesebb mint kétszáz év alatt eljutott a pilóta nélküli repülőgépek használatáig, a korszakalkotó technológiák térnyerésének eredményeképp pedig ma már a mesterséges intelligencia (MI) által vezérelt felderítő vagy akár csapásmérő eszközök alkalmazásának lehetőségei is felmerülnek, azok minden jogi és erkölcsi-etikai aspektusával együtt.[4]

Jelenkorunk dinamikusan változó biztonsági környezetének folyamatait és ezzel együtt a NATO biztonságfelfogását alapjaiban határozza meg a kiéleződő technológiai verseny, amely kiterjed olyan korszakalkotó technológiák (EDT) területére, mint az MI, a kvantumtechnológia, az autonóm rendszerek, a biotechnológia, de a katonai biztonság szempontjából szintén meghatározó szerepet kap az űr-, illetve a rakétatechnológia is. Továbbá a hadviselés hibridizációja és a kibertéri fenyegetések is egyfajta fokozó tényezőként *(threat multiplier)* befolyásolják a nemzetközi biztonsági környezet dinamikáit.[5]

Ezen új technológiai vívmányok megjelenése, folyamatos és gyors ütemű fejlődése bizonytalanságot és kiszámíthatatlanságot eredményez, aminek következtében nehéz

[2] O'Connell 1963.
[3] NATO Strategic Concept 2022: 1.
[4] NATO Science and Technology Organization 2025: 13, 17.
[5] NATO Science and Technology Organization 2025: 10–14.

feladattá válik a NATO és más nemzetközi szereplők számára is annak meghatározása, hogy pontosan milyen kihívások megoldására kell felkészülni és mikor, valamint hogy az elrettentés és a védelem bevett gyakorlatait miképp igazítsák a technológia által egyre inkább befolyásolt biztonsági környezethez.[6]

Az utóbbi gondolatmenetből következő lehetséges fejlődési, fejlesztési irányvonalakhoz támpontot képezhet az ellenlábasok, vetélytársak tevékenységének figyelemmel kísérése. Továbbá az ezen ellenérdekelt felek által végrehajtott kibertéri vagy hibrid jellegű támadások felfedhetik a védelem azon réseit, amelyekre a jövőben nagyobb fókuszt kell helyezni ahhoz, hogy továbbra is szilárd pilléreken álljon a külső fenyegetések elhárítására létrehozott védelmi rendszer. A NATO számára a 2022-es stratégiai koncepció alapján jelenleg a legnagyobb fenyegetést Oroszország jelenti, de kihívás szintjén megjelenik Kína is, amely hibrid és kiberműveletekkel, egyre élesebb retorikával és dezinformációs kampányokkal igyekszik aláásni a NATO-szövetségesek biztonságát.[7]

Ez az elemzés arra keresi a választ, hogy a NATO hogyan értékeli a gyors ütemű technológiai fejlődés hatásait és a technológiai verseny kiéleződését, valamint hogyan próbálja megőrizni a biztonság fenntartásához szükséges technológiai fölényt. Először azonban meg kell vizsgálni, milyen események vezettek a jelenleg zajló folyamatokhoz.

A biztonság technológiai aspektusainak felértékelődése

Romló biztonsági környezet

A bevezetőben már szóba került, hogy a technológiai fölény megszerzése és megtartása mindig is fontos cél volt, legyen szó háborús vagy békeidőszakról. Napjainkban mégis különös hangsúly helyeződik az innovációra, a képességfejlesztésre és a civil szférában működő vállalatok által fejlesztett technológiák minél gyorsabb ütemű adaptálására, ennek érdekében a NATO is kialakította, illetve folyamatosan bővíti a szükséges csatornáit.[8]

Ahhoz, hogy jelenkorunkban ennyire fontossá váljanak a biztonság technológiai aspektusai, számos olyan tényező hozzájárult, amely a 2000-es, de inkább a 2010-es években az instabilitás és a bizonytalanság felé terelte a nemzetközi biztonsági környezetet. Egyike ezen tényezőknek Oroszország ukrajnai inváziója, amelyet különböző biztonságelméletek eltérő megközelítéssel magyaráznak. A liberális iskola hisz az emberi értelem felülkerekedésében és abban, hogy a nemzetközi intézmények által átszőtt, interdependens világban csak egy irracionálisan gondolkodó aktor képes elindítani egy ilyen jellegű kontraproduktív háborút.[9] A realista iskola ezzel szemben, alapozva John H. Herz amerikai nemzetközi szakértő elméletére a biztonsági dilemmáról, egyáltalán

[6] NATO Science and Technology Organization 2025: 14.
[7] NATO Strategic Concept 2022: 4–5.
[8] Az említett csatornákat, mint például a NATO DIANA és a NATO *Space Front Door* kezdeményezést vagy a Gyors ütemű adaptációs cselekvési tervet (*Rapid Adoption Action Plan,* RAAP) a tanulmány egy későbbi fejezetében mutatom be.
[9] Greminger–Vestner 2022: 9.

nincs meglepve attól, hogy egy magát fenyegetve érző állam a saját biztonságának növelése, illetve a túlélés érdekében háborút kezdeményez.[10] Végül, de nem utolsósorban a konstruktivisták a mélyen gyökerező okokban, indentitásbeli kérdésekben és fenyegetettségpercepciókban keresik a háború okait.[11] Akárhonnan is közelítjük meg, az invázió visszahozta Európába a háború valóságát, ami a NATO-szövetségeseket is a korábbiaknál erőteljesebben ösztönzi, hogy fejlesszék katonai képességeiket, ami egyébként is alapkötelezettségük a washingtoni szerződés 3. cikke alapján.[12]

Oroszország mellett a NATO szemszögéből nézve fokozatosan, de leginkább amerikai irányból felerősítve megjelent Kína is mint kihívás. Ennek egyik oka Kína hihetetlenül gyors gazdasági fejlődése,[13] amelyhez társul a világgazdasági folyamatok feletti ellenőrzés egyre szélesebb körű megszerzésére való törekvés is. Emellett a Tajvannal való újraegyesítés célkitűzése, a dél-kínai-tengeri biztonsági igényei[14] és azon nyugati, elsősorban amerikai percepciók[15] is hozzájárulnak a jelenlegi folyamatokhoz, amelyek szerint Kína a világrend átalakítására és a világ vezető szerepének átvételére, valamint a nyugati országok által lefektetett nemzetközi rend átformálására vagy leváltására törekszik.

Technológiai aspektusok

Az indikátorokat még hosszan lehetne sorolni, viszont a téma szempontjából a legfontosabb megemlíteni azon technológiai aspektusokat, amelyek különösen a 2010-es, illetve mindinkább a 2020-as években kerültek előtérbe. 2007-ben jól körvonalazódott, hogy a kibertér szerepe a jövő hadviselésében fontos szerepet fog betölteni.

Miután az észt kormány egy tallinni szovjet hősi emlékmű eltávolításáról és áthelyezéséről döntött, 2007. április 27. és május 27. között folyamatos kibertámadások érték a különböző kritikus infrastruktúrákat, bankrendszereket, kormányzati rendszereket, ami így először mutatta be a világ számára, hogyan is nézhet ki egy kibertérben vívott háború.[16] Az egy évvel később bekövetkezett, öt napig tartó orosz–grúz háború szintén erős jelzés volt, hogy foglalkozni kell a kérdéssel, hiszen ez volt az első alkalom, hogy a kibertéri műveleteket az egyéb, valós térben zajló katonai műveletekkel összehangoltan hajtották végre.[17] Ezt követően különösen a 2010-es évek közepétől erősödött fel a kibertér jelentősége, amiben nagy szerepe volt a Krím félsziget Oroszország általi 2014-es annexiójának is, amely során egyrészt kibertámadások is részét képezték az orosz műveleteknek, másrészt széles körben megjelent

[10] Greminger–Vestner 2022: 10.
[11] Shahir–Boghairy 2024: 6.
[12] Az Észak-atlanti (washingtoni) szerződés (1949. április 4.) 3. cikke kimondja, hogy a szövetségeseknek egyénileg és együttműködve is fejleszteni kell kollektív védelmi képességeiket.
[13] 1980 és 2020 között Kína GDP-je 400 milliárd USD-ről 15 000 milliárd USD-re nőtt, 2025-ben pedig már 18 000 milliárd USD. World Bank Group [é. n.].
[14] Ministry of National Defense of the People's Republic of China: Defense Policy.
[15] *United States National Security Strategy 2022* 2022: 8.
[16] Szentgáli 2013: 78.
[17] Szentgáli 2013: 79.

a nyugati szakértők szóhasználatában egyébként már korábban is létező *hibrid hadviselés* fogalma, amelyet az újszerűnek ható orosz hadviselés leírására alkalmaztak.[18]

A hibrid hadviselés definiálására hazánkban több kísérlet született. Resperger István definíciója alapján a hagyományos reguláris és az irreguláris hadviselés puha, közepes és kemény módszereinek rugalmas alkalmazását jelenti a hibrid hadviselés.[19] Porkoláb Imre szerint a hibrid hadviselés az irreguláris hadviselés egy újabb fejlődési lépcsőfokát jelenti.[20]

A NATO által 2024-ben kiadott, hibrid fenyegetésekre és hadviselésre vonatkozó iránymutató dokumentum alapján pedig a hibrid hadviselés nem más, mint a hatalom kemény, puha és okos eszközeinek *(hard, soft, smart power)* egy rosszindulatú állami vagy nem állami szereplő általi használata háborús és politikai célok elérése érdekében.[21] A hibrid hadviselés keretében katonai és nem katonai eszközök széles skálája alkalmazható, amelyek végrehajtása nyíltan és rejtett módon egyaránt zajlik a szürkezónában, ahol elmosódik a határ háború és béke között. Ezen hadviselési módszernek fontos elemeivé váltak a kibertéri műveletek, kritikus infrastruktúrák elleni támadások, dezinformációs kampányok, manipulált internetes tartalmak a társadalmi elégedetlenség szítására, amelynek az utóbbi időben fontos elemévé vált egy másik technológiai terület, az egyik korszakalkotó technológia, a mesterséges intelligencia.[22]

Az MI képeket, videókat, nyilatkozatokat képes manipulálni, ami hozzájárulhat a társadalom bomlasztásához, de ezen túlmenően is számos olyan felhasználási területe van, amely valamilyen módon érinti az átfogó biztonságot. Az MI képes lehet felgyorsítani vagy befolyásolni a döntéshozatali folyamatot, akár negatív irányba is, illetve katonai szempontból fontos szerepet játszhat a felderítés, az információszerzés és akár a csapásmérés folyamatában is. Ebből adódóan az MI, illetve az autonóm rendszerek fejlesztése a nemzetközi technológiai verseny kiemelt területének számít, és jelentős mértékben befolyásolhatja a jövő hadviselését, valamint a nemzetközi biztonsági környezet folyamatait.[23]

A MI-hez hasonlóan fontos terület a kvantumtechnológia is, amely a tudományos és katonai célú rendszerek fejlődésében is előrelépést hozhat, elsősorban az adatfeldolgozás, -gyűjtés és -biztonság, valamint a szenzortechnológia-fejlesztés és az anyagkutatás területén.[24]

Végül, de nem utolsósorban fontos eleme a technológiai versenynek és a biztonság technológiai aspektusainak az űr, azon belül is a Földről indítható műhold elleni fegyverrendszerek, a műholdról indítható rakéták, a jelzavaró eszközök és egyéb katonai űrképességek, amelyek területén egyre fokozódó verseny várható.[25]

Utóbbi gondolatmenet felidézheti Ronald Reagan amerikai elnök 1983-ban meghirdetett stratégiai védelmi kezdeményezését (*Strategic Defense Initiative,* SDI),[26]

[18] JÓJÁRT 2020: 6.
[19] JÓJÁRT 2020: 6.
[20] JÓJÁRT 2020: 6.
[21] NATO Hybrid Threats and Hybrid Warfare Reference Curriculum 2024: 17.
[22] NATO Hybrid Threats and Hybrid Warfare Reference Curriculum 2024: 26.
[23] NATO Science and Technology Organization 2025: 16–20.
[24] NATO Science and Technology Organization 2025: 16–20.
[25] NATO Science and Technology Organization 2025: 12–14.
[26] U.S. Department of State 1983.

amelyet csillagháborús tervként is szokás emlegetni. A terv egy olyan rakétavédelmi rendszert vázolt fel, amelynek célja az orosz ballisztikus rakéták korai megsemmisítése volt, mielőtt még azok elérhetnék az Egyesült Államok és szövetségeseik területét.[27] Az új űrverseny és az űrerők építése napjainkban hasonló jellegű törekvésekre épülhet.

Összességében tehát számos olyan technológiai aspektus felsorolható, amely valamilyen módon hat a nemzetközi szereplők biztonságfelfogására és fenyegetettségpercepcióira, amelyek kiegészítik a politikai célokat és a hatalmi törekvéseket, ezzel mintegy fenyegetésfokozó tényezőként hozzájárulva a nemzetközi biztonsági környezet instabil, bizonytalan jellegéhez.[28] A következőkben kifejezetten a NATO szemszögéből kerül górcső alá, hogy ezen új technológiai tényezők, új típusú fenyegetések és kihívások miként formálták a NATO biztonságfelfogását.

Technológia és a NATO biztonságfelfogása

Stratégiai irányvonalak

A NATO stratégiai koncepciói jó indikátorok ahhoz, hogy le lehessen képezni a szövetség aktuális prioritásait és biztonságfelfogását. A koncepciók feladata meghatározni a NATO hosszú távú célkitűzéseit, valamint a szervezet jellegét, továbbá számba venni a nemzetközi biztonsági környezet aktualitásait, amelyek alapján később feladatok szabhatók a kitűzött célok elérése érdekében. A koncepciók iránymutatást adnak a haderők fejlesztési irányaival kapcsolatban, vagyis összességében olyan létfontosságú dokumentumok, amelyek segítenek a NATO-nak alkalmazkodni a megváltozott biztonsági környezethez.[29]

A szervezetnek jelenleg a nyolcadik, 2022-ben elfogadott stratégiai koncepciója van érvényben, amely részletes útmutatást tartalmaz a technológia biztonsági aspektusainak vonatkozásában, viszont az adaptációs folyamatok és a biztonsági környezet változásának szemléltetéséhez egy rövid kitekintés erejéig érdemes visszatérni a hetedik, vagyis a 2010-es stratégiai koncepcióhoz. Ez az első stratégiai koncepció, ahol a technológiai fejlődés hatásainak részletesebben kifejtett aspektusai is megjelennek, mint például a lézerfegyverek, az elektronikai hadviselés, valamint az űrt érintő technológiai kihívások.[30] A 2010-es stratégiai koncepció tulajdonképpen megágyazott olyan későbbi eseményeknek, mint a kibertér és az űr hadműveleti térré nyilvánítása. Ennek ellenére mégis ki lehet jelenteni, hogy a dokumentum a 2022-es stratégiai koncepcióhoz képest jóval kisebb teret és figyelmet szentel a technológiai fejlődés – és verseny – biztonsági környezetre gyakorolt hatásainak.[31]

A Madridban elfogadott 2022-es koncepció nemcsak több teret enged a biztonság technológiai fejlődéshez és versenyhez kapcsolódó színterének, de mivel a 49

[27] U.S. Department of State 1983.
[28] NATO Defense College 2022: 4.
[29] Szenes – Siposné Kecskeméthy 2019: 28.
[30] The Alliance's Strategic Concept 2010: 12.
[31] The Alliance's Strategic Concept 2010: 12.

bekezdésből legalább kilencben megjelenik valamilyen formában, elmondható, hogy napjainkra kulcsfontosságúvá vált a terület a NATO biztonságfelfogásában.[32] A dokumentum ráadásul már nemcsak általánosságban említi meg a technológiai fejlődés egyes elemeit, hanem összeköti azokat a szövetségesek számára fenyegetést vagy kihívást jelentő nemzetközi szereplőkkel is.

Szó esik a terrorszervezetek fejlett technológiához jutásának veszélyeiről, amelynek következtében a terroristák távoli célpontokat is könnyebben elérhetnek, illetve pontosabb és halálosabb tevékenységet folytathatnak.[33] Oroszország és Kína kapcsán megjelennek az ártó szándékú hibrid jellegű, illetve kibertéri műveletek, amelyekkel megpróbálják gyengíteni és destabilizálni a NATO-t, továbbá aláásni a jelenlegi, nyugati értékeken és érdekeken alapuló nemzetközi rendet.[34] Megjelennek továbbá a kritikus infrastruktúrák fenyegetései, valamint az érzékeny információk megszerzésére irányuló törekvések és a kormányzati rendszerekbe való betörés és károkozás veszélyei.[35] Végül, de nem utolsósorban a koncepció kijelenti, hogy a stratégiai versenytársak a NATO űrképességeinek fejlesztését és a civil, valamint katonai infrastruktúrák zavartalan működését is akadályozni igyekeznek, vagyis összességében komoly kihívást jelent az erre irányuló tevékenységek elleni megfelelő védelem megteremtése a NATO számára, éppen ezért nagy hangsúlyt kell fektetni az ez irányú képességek fejlesztésére.[36]

Hasonlóképpen, a dokumentum az EDT-k kapcsán is lefekteti, hogy ezen új technológiák azon túlmenően, hogy lehetőségeket hordoznak magukban, kockázatokat is rejtenek, és a sikeres – vagy sikertelen – adaptálásuk növekvő mértékben befolyásolja majd a csatatéren zajló események kimenetelét.[37] Éppen ezért a technológiai fölény megszerzése és megtartása a riválisokkal szemben a NATO kiemelt feladatainak egyike annak érdekében, hogy továbbra is biztosítani tudja a szövetségesek számára a külső fenyegetésekkel szembeni védelmet, ezzel megugorva az adaptáció egy újabb lépcsőfokát.[38]

Reakció és adaptáció

A NATO tehát most már több mint 75 éve rajzolja fel az új viszonyokhoz való alkalmazkodás történetét. A folyamatos megújulási és fejlődési képességének köszönhetően a NATO mind a mai napig releváns kollektív védelmi szervezet tudott maradni minden nehézség és válság ellenére, és bízni lehet benne, hogy ez a jövőben is így marad. A stratégiai koncepciók tartalmainak ismertetését követően, mielőtt részletesebben is megvizsgáljuk, hogy pontosan milyen eszközökön keresztül igyekszik a NATO adaptálni az új technológiákat, érdemes tömören áttekinteni azt is, hogy milyen folyamatok mentek végbe a 2010-es és a 2022-es stratégiai koncepció között, ami indokolttá tette, hogy a szövetségesek nagyobb figyelmet fordítsanak ezen fontos területekre.

[32] NATO Strategic Concept 2022.
[33] NATO Strategic Concept 2022: 4.
[34] NATO Strategic Concept 2022: 5.
[35] NATO Strategic Concept 2022.
[36] NATO Strategic Concept 2022.
[37] NATO Strategic Concept 2022.
[38] NATO Strategic Concept 2022: 1–3.

Kezdve a sort a kibertéri támadásokkal, valójában már a 2007-es észtországi incidens után döntöttek a szövetségesek védelmi miniszterei az Észak-atlanti Tanács ülésén arról, hogy össze kellene hangolni a tagországok kibervédelmi tevékenységeit,[39] nem sokkal később, 2008 januárjában a NATO elfogadta a *Kibervédelmi irányelv*et *(Policy on Cyber Defence)*.[40] Ugyanezen évben a szövetség megalapította a Kooperatív Kibervédelmi Kiválósági Központot (Cooperative Cyber Defence Centre of Excellence, CCDCOE), amelynek fő feladatává a kiberbiztonsággal, kibertéri műveletekkel kapcsolatos kutatás és fejlesztés, valamint oktatás és iránymutatás vált.[41]

Részben a szervezethez köthető a későbbi *Tallinni kézikönyv* első változatának megírása is, ugyanis a kézikönyvet a CCDCOE által meghívott mintegy húsz szakértő állította össze 2009 és 2012 között. A kézikönyv a kiberháborúra alkalmazandó nemzetközi jogi aspektusokat hivatott tisztázni.[42]

A következő jelentős előrelépés 2010-ben történt, mégpedig egy újabb jelzésértékű kibertámadás keretében, amely ismét „eszkalált" a korábbi tapasztalatokhoz képest. Ez volt a feltehetően amerikai–izraeli eredetű Stuxnet nevű számítógépes féreg okozta incidens, amely során a kártevő számítógépes program jelentős károkat okozott az iráni nukleáris létesítményekben, megsemmisítve az urándúsításhoz elengedhetetlen centrifugák legalább egyötöd részét.[43] A kibertámadások így fokozatosan elkezdtek összefonódni a hibrid fenyegetésekkel, illetve hadviseléssel, amelyek különösen a már korábban említett 2014-es krími annexió után kerültek előtérbe.

A krími események hatására a NATO fel is vette a listájára a hibrid fenyegetések és a hibrid hadviselés jelentette kihívásokat, és az alig néhány hónappal későbbi walesi csúcstalálkozón már az ezen fenyegetések elhárítására irányuló intézkedések minél korábbi megkezdését sürgették. A walesi csúcstalálkozón a NATO bevonta a tagállamok ellen indított kibertámadásokat a kollektív védelem elve, vagyis a washingtoni szerződés ötödik cikkének érvényessége alá.[44] Csak érdekességképpen illik megemlíteni, hogy ez a csúcstalálkozó volt az is, ahol a tagállamok megegyeztek abban, hogy azon országok, amelyek nem érik el 2014-ben a védelmi kiadások 2%-os GDP-arányos mértékét, a következő évtizedben legalább megközelítik majd ezt a célkitűzést.[45] Utóbbi gondolatmenethez kapcsolódóan 2025-ben a hágai csúcstalálkozón a szövetségesek amerikai nyomásra új védelmi költségvetési célt fogadtak el, amelynek értelmében 2035-ig GDP-arányosan 5%-ra kell növelniük védelmi kiadásaikat. Ezen új célkitűzés alapján egyrészt 3,5%-ot kell a hagyományos értelemben vett védelmi célú kiadásokra fordítani, míg a fennmaradó 1,5% a védelmi célú törekvéseket támogató egyéb beruházásra is fordítható, például infrastruktúra-fejlesztésre.[46]

Visszakanyarodva a hibrid és kiberfenyegetésekhez, a NATO a 2016-os varsói csúcstalálkozón műveleti térré nyilvánította a kiberteret, valamint a szövetség az Európai Unióval is elkezdte szorosabbra fűzni együttműködését, amelynek egyik

[39] NATO 2007.
[40] NATO 2024a.
[41] Paráda 2018: 3–13.
[42] Cooperative Cyber Defence Centre of Excellence [é. n.].
[43] Bránya 2019: 18–21.
[44] NATO 2014.
[45] NATO 2014.
[46] NATO 2025b.

eredménye lett a 2017-ben létrehozott Hibrid Fenyegetések Elleni Európai Kiválósági Központ (The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE), amelynek feladata az Európát fenyegető kibertámadások, illetve a dezinformációs műveletek elemzése, valamint a részt vevő országok felkészítése a hibrid fenyegetések elhárítására, kezelésére.[47]

Utóbbi történések kapcsán érdemes megemlíteni a NATO reakcióinak kiváltó okait. A kibertér behálózza a világot, és a rendkívüli ráutaltság révén, mondhatni, az internet kritikus infrastruktúrává vált, amelynek hosszú távú kiesése vagy akár a benne zajló különböző műveletek súlyos következményekkel járhatnak egy adott államra vagy akár egy egész kontinensre nézve.[48] Konkrét példákkal szemléltetve elsőként megemlíthető az Egyesült Államok Nitro Zeus haditerve, amely eredetileg Irán ellen irányult arra az esetre, ha a közel-keleti ország túl közel kerülne az atombomba kifejlesztéséhez. A terv keretében az Egyesült Államok a támadás első lépéseként az interneteléréstől fosztaná meg Iránt az elektronikai hadviselés eszközeivel elektromos hullámtartomány, így megbénítva az ország teljes infrastruktúráját, valamint védelmi rendszereit, ezt követően pedig folyamatos kibertámadások kíséretében indítaná meg légi és szárazföldi műveleteit.[49]

Említhető továbbá az a 2015-ös ukrajnai eset is, amikor egy kibertámadás következtében legkevesebb 250 000 ember maradt áram nélkül huzamosabb ideig,[50] de a dezinformáció oldaláról nézve az is felvethető, amikor 2021. január 6-án a Donald Trump amerikai elnökről szőtt és az amerikai társadalom egy részét befolyásoló internetes konspirációs teóriák hatására halálos áldozatokkal járó ostromba torkollt a Washington D.C.-ben található Képviselőház előtti tüntetés, amihez nagyban hozzájárult az amerikai elnök buzdítása is, aki választási csalásról beszélt.[51] A kibertér tehát a teljesség igénye nélkül lehetőséget biztosít társadalmi bomlasztásra és infrastruktúrák elleni támadásokra is. 2012-ben Leon Panetta, az Egyesült Államok akkori védelmi minisztere arról beszélt, hogy a 21. században akár még egy kiber-Pearl Harbor is előfordulhat.[52]

A hibrid, illetve kiberfenyegetéseken túlmenően ugyanakkor más technológiai aspektusokat is meg kell említeni, amelyek ugyancsak fontos pillérei lehetnek a jövő hadviselésének, így a NATO számára is elengedhetetlen, hogy reagáljon rájuk. Ezen technológiák az EDT-k vagy korszakalkotó technológiák, illetve részint idekapcslódóan az űrképességek is. Noha alapvetően a hibrid és kibertevékenységek kapcsolatban állhatnak ezen új technológiákkal, mégis, mivel viszonylag friss jelenségekről van szó, érdemes őket önálló alfejezetben ismertetni.

[47] Hybrid CoE [é. n.].
[48] Haig–Kovács 2012: 40, 121.
[49] Hofstetter 2020: 172.
[50] Peterson 2016.
[51] Capitol Riots Timeline: What Happened on 6 January 2021? 2021.
[52] Daily Report: Panetta Warns of Dire Threat of Cyberattack on U.S. 2012.

Új technológiák adaptációja

2019-ben a NATO az űrt is beemelte a műveleti terek listájába, ezzel ötre bővítve azt (szárazföld, levegő, tenger, kibertér, űr).[53] Az Egyesült Államok ugyancsak 2019-ben felállította az Űrerőket, amely külön haderőnemnek számít. Oroszország összevont Légi- és Űrerőkkel operál, Kína pedig 2024-ben hozta létre a Stratégiai Támogató Erők haderőnem egyik utódágazataként az Űrműveleti Erőket.[54]

Az űrképességek fejlesztése egyre fontosabbá válik a biztonság, illetve a hadviselés szempontjából, ezért ez kiemelt területe napjaink technológiai versenyének. 2025 júliusára Kínának már 1189 műholdja keringett a Föld körül, amelyek közül legalább 500 képes hírszerzési, megfigyelési, felderítési feladatok végrehajtására (*intelligence, surveillance, reconnaissance,* ISR).[55] Ez a közel 1200 műhold ezerrel több, mint amivel Kína 2015-ben rendelkezett, és kitűzött cél, hogy 2030-ra 15 000 kínai műhold keringjen a bolygó körül.[56]

Ezen túlmenően, ami a katonai célú felhasználást illeti, Kína erőteljesen fejleszti az űrelhárító *(counter-space)* képességeit, hogy képes legyen zavarni vagy akár megsemmisíteni az ellenséghez tartozó műholdakat egy esetleges háború esetén.[57] A tudományba és a technológiába (*science and technology,* S&T) ölt hatalmas erőforrások révén pedig (a GDP legalább 2,3%-a) Kína több, az űrhöz kapcsolódó technológiai fejlesztési területen is élen jár, így például a kvantumtechnológia területén.[58] Oroszország és az Egyesült Államok hasonlóképpen fejlesztik műholdelhárító képességeiket és/vagy műholdról indítható, földi célpontok ellen is alkalmazható fegyverrendszereiket.[59] Az amerikai törekvéseknél külön kiemelendő a 2025 tavaszán bejelentett Aranykupola: olyan fejlett rakétavédelmi rendszer lenne, amely űrbe telepített komponenseket (szenzorok, elfogórakéták) is magában foglalna.[60]

A fentiekből adódóan a NATO-nak is reagálnia kell az űrben zajló folyamatokra, hogy ebben a műveleti térben is képes legyen biztosítani az elrettentést. Ehhez az egyik legfrissebb irányadó dokumentum a 2025 februárjában bejelentett *Kereskedelmi űrstratégia (NATO Commercial Space Strategy),* amelynek legfőbb eleme, hogy a NATO-nak meg kell erősítenie a kapcsolatát a kereskedelmi űripari szereplőkkel ahhoz, hogy az együttműködések révén hatékonyabban tudja adaptálni a kereskedelmi szféra (civil szektor) új innovációit.[61] Ezzel a dokumentummal szoros kapcsolatban áll a *NATO Space Front Door (Kapu az űrre)* kezdeményezés, amelynek célja amerikai mintára létrehozni egy fórumot a kereskedelmi szektor szereplői és a NATO számára, ahol a kereslet találkozhat a kínálattal, ezáltal hatékonyabbá tenni az innovációs és adaptációs folyamatokat.[62]

[53] NATO 2019.
[54] United States Space Force [é. n.].
[55] United States Space Force [é. n.].
[56] United States Space Force [é. n.].
[57] United States Space Force [é. n.].
[58] NATO Science and Technology Organization 2025: 18.
[59] United States Space Force [é. n.].
[60] Lockheed Martin [é. n.].
[61] NATO 2025a.
[62] Waterman 2025.

Végül, de nem utolsósorban az űr kapcsán meg kell említeni egy fontos mérföldkövet, a 2024-es washingtoni NATO-csúcsot, amely egyébiránt egybeesett a szövetség 75. születésnapjával is. A csúcson elfogadtak egy új, multitérműveletekre *(multi-domain operations)* vonatkozó koncepciót, amelynek lényege az űr hatékony integrálása a szárazföldi, légi, tengeri és kibertéri műveletek mellé, ami azt jelenti, hogy mind a tervezésbe, mind pedig a jövőbeli közös gyakorlatokba integrálják az űrt mint műveleti teret is.[63] A célkitűzés, hogy a szervezet 2030-ra már képes legyen mind az öt műveleti teret érintően összehangolt műveleteket végrehajtani.[64]

Az űr mellett ugyanakkor mindenképpen reflektálni kell a mesterséges intelligenciára és az autonóm rendszerek kérdéskörére. Az olyan új és korszakalkotó technológiák alkalmazása, mint az MI, illetve az autonóm rendszerek, nemcsak új lehetőségeket kínál a védelem és a hadviselés terén, hanem új fenyegetéseket is generál. Az ilyen technológiák gyors fejlődése és elterjedése lehetővé teszi az állami és nem állami szereplők számára, hogy hatékonyabban és rugalmasabban reagáljanak a biztonsági kihívásokra, ugyanakkor új támadási felületeket is teremt.[65] Elég csak a kínai tiszta technológiák (akkumulátorok, napelemek, áramátalakítók) világpiaci dominanciájára és ennek lehetséges következményeire gondolni. Európában egyértelműen a kínai technológia az uralkodó ezen (tiszta) zöldtechnológiákban,[66] amelyek okosítása vagy akár egy esetleges jövőbeli MI általi vezérlése súlyos kockázatokat rejt magában. Ezen technológiák, különösen az áramátalakítók a napelemek esetében, rá vannak kötve az európai elektromos hálózatra, és már most is rendelkeznek távvezérlési funkciókkal, amelyek lehetővé teszik, hogy akár a vezérlő, akár egy kiberbűnözői csoport átállíthassa vagy rosszabb esetben elpusztíthassa azokat.[67] Ezenfelül az MI alkalmazása nemcsak technológiai, hanem társadalmi és etikai kérdéseket is felvet. Az algoritmusok döntései gyakran átláthatatlanok és nem feltétlenül vezetnek a probléma megoldása felé, ami különösen aggasztó lehet, ha az egyenletben emberéletek is helyet kapnak. Emiatt egyfajta megbízhatatlanság alakul ki, amire rárakódik még a gépi tanulás rendszereinek torzítása és manipulálhatósága, ami komoly kockázatokat hordozhat magában, más szóval lehetőséget biztosít a szabotázsakciók végrehajtására is.[68] Összességében az MI egyelőre nem kiforrott technológia, de katonai alkalmazás szempontjából egyértelműen az egyre fejlettebb autonóm rendszerek megalkotása a cél, ami segítheti a célpontfelismerést és -semlegesítést, valamint a döntéshozatalt.[69]

Mindezzel együtt az MI megkerülhetetlen, és a NATO hosszú távú technológiai előre jelző jelentése alapján méltán kerül a legfontosabb területek közé, ahol a stratégiai verseny zajlik. A teljesség kedvéért, a listába tartozik még az MI-n kívül az űr, a kvantumtechnológia, a kiberképességek, illetve az egészet átfogóan a hadviselés hibridizációja is komoly kihívás, különösen a kritikus infrastruktúrákra jelentett fenyegetések révén.[70]

[63] NATO 2024b.
[64] NATO 2024c.
[65] NATO Science and Technology Organization 2025: 16–18.
[66] Green Dealflow 2025.
[67] Langerová 2025.
[68] Hofstetter 2020.
[69] NATO Science and Technology Organization 2025: 16–18.
[70] NATO Science and Technology Organization 2025: 10–18.

Utóbbiakat kiegészítve, a NATO az energiaellátás hatékonyságának növelésére, az újgenerációs kommunikációs technológiákra, a hiperszonikus rendszerekre, a biotechnológiára és a gyártási-előállítási folyamatok területén jelentkező új típusú technológiákra (például 3D-nyomtatás) is nagy hangsúlyt fektet, és külön-külön stratégiákat fejleszt. Ezen technológiák integrálása a NATO védelmi tervezésébe rendkívül lényeges, éppen ezért fontos elemeivé váltak az éves NATO-csúcstalálkozóknak is, különösen az űrtechnológia, az MI és az autonóm rendszerek.[71]

Ami az említett technológiákat illeti, ugyan az űr kapcsán már említettük a *NATO Space Front Door* kezdeményezést, a szinte minden terület technológiai innovációs folyamatait érintő DIANA programról[72] *(Defence Innovation Accelerator for the North Atlantic, Észak-atlanti védelmi innovációs akcelerátor)*[73] mindenképpen szót kell ejteni. A DIANA program elindításáról 2021-ben állapodtak meg a NATO-szövetségesek. A program lehetővé teszi az innovátorok számára a NATO technológiai infrastruktúrájához, tesztközpontjaihoz való hozzáférést, ezzel, valamint mentorálással támogatva munkájukat. A DIANA programom belül már több mint 200 gyorsító- és tesztközpontot hoztak létre a tagállamok területein.[74] Érdekességképpen, Magyarországon 2023-ban jött létre a Védelmi Innovációs Kutatóintézet, amely szervezetnek kiemelt céljai közé tartozik a magyar haderő képességfejlesztéseinek támogatásán túl, hogy beilleszkedjen a NATO innovációs ökoszisztémájába.[75] A DIANA rendkívül fontos összekötő elem a NATO és a kereskedelmi szféra innovátorai között, és jelentős a szerepe a NATO adaptációs folyamataiban, amelyek célja a stratégiai koncepcióban lefektetett technológiai előny megtartása a NATO technológiával kapcsolatos jelenkori biztonságfelfogásának megfelelően.[76]

Összegzés

2025-ben a NATO kiadta a 2045-ig tartó, vagyis 20 évre szóló jelentését a biztonságot és a védelmet formáló tudományos és technológiai trendekről. Ezen jelentés alapján a következő 20 évben az alábbi – a korábbiakban is fejtegetett – trendek határozzák majd meg a szövetség technológiai versennyel kapcsolatos gondolkodását: a mesterséges intelligencia és a kvantumtechnológia fejlesztésére irányuló verseny, az űrtechnológia, a hadviselés hibridizációja, a kibertérbeli kihívások, a biotechnológia forradalma, az erőforrások elosztása, a technológiai függőségek és integrációs folyamatok, valamint általánosságban véve a technológiai, illetve a hatalmi-stratégiai verseny egyes aspektusai.[77]

A 20 évre szóló jelentésben feltüntetett trendekből jól kivehetők a NATO számára hangsúlyos pontok, amelyekre a jövőben a szövetség koncentrálni akar. Kérdés, hogy vajon az Egyesült Államok és Európa hogyan tud majd együttműködni a jelenlegi

[71] NATO 2024b.
[72] NATO 2025c.
[73] Porkoláb–Hőnich 2021: 21.
[74] NATO 2025c.
[75] Porkoláb–hennel–hegedűs 2023: 47–48.
[76] NATO Stratégiai Koncepció 2022.
[77] NATO Science and Technology Organization 2025.

politikai csatározások fényében, illetve hogy a szövetség egységes tud-e maradni a következő 20 évben. A felsorolt elemek, amelyek mentén a NATO a jövőt tervezi, úgy gondolom, önmagukban megérnek egy külön tanulmányt, ezen írás azonban elsősorban a technológiai vívmányok, a technológiai verseny kiéleződésére, illetve a NATO adaptációs folyamatainak tömör bemutatására fókuszált.

A technológiai fejlődés egyes aspektusai, legyen szó a kibertéri vagy az EDT-kkel kapcsolatos területekről, egyértelműen új lehetőségeket és egyúttal kockázatokat is hordoznak magukban. Ami a mezőgazdaságban lehetőség, például az MI-vezérelt öntözőrendszer, az a katonai oldalon a kibertámadások kiemelt célpontjává válhat, csakúgy, mint a távolról vezérelhető kínai napkollektor-kiegészítők. Utóbbira példa lehet az a 2023-as németországi eset, amikor 800 napelemes rendszer ment tönkre egy félresikerült szoftverfrissítés miatt.[78] Az új technológiák számtalan kockázatot hordoznak magukban, különös tekintettel a kritikus infrastruktúrákra, azon belül is az energiahálózatot érintően. Éppen ezért fontos, hogy a NATO megfelelő módon adaptálja és alkalmazza az új technológiákat, hogy fel tudjon készülni az ilyen irányú támadások kivédésére, ezzel biztosítva a tagállamai biztonságát és legfőbb feladatát, a kollektív védelmet.

Felhasznált irodalom

Brányi Bence (2019): Szemelvények a kiberhadviselés jelenéből. Az informatika uralta haderők sebezhetőségének érzékeltetése öt példán keresztül. III. rész. *Haditechnika,* 53(1), 18–21. Online: https://doi.org/10.23713/HT.53.1.04

Capitol Riots Timeline: What Happened on 6 January 2021? *BBC,* 2023. augusztus 2. Online: https://www.bbc.com/news/world-us-canada-56004916

Cooperative Cyber Defence Centre of Excellence [é. n.]: *The Tallinn Manual.* Online: https://ccdcoe.org/research/tallinn-manual/

Daily Report: Panetta Warns of Dire Threat of Cyberattack on U.S. *The New York Times,* 2012. október 12. Online: https://archive.nytimes.com/bits.blogs.nytimes.com/2012/10/12/daily-report-panetta-warns-of-threat-of-cyberattack-on-u-s/

Enkhardt, Sandra (2023): Around 800 Sungrow Batteries Affected by Outage in Germany. *PV Magazine,* 2023. március 17. Online: https://www.pv-magazine.com/2023/03/17/around-800-sungrow-batteries-affected-by-outage-in-germany/

Észak-Atlanti (Washingtoni) Szerződés (1949. április 4.). Online: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=hu

Green Dealflow (2025): *China's Renewable Energy Strategy?* Online: https://green-dealflow.com/can-europe-compete-with-chinas-renewable-energy-strategy

Greminger, Thomas – Vestner, Tobias (2022): *The Russia-Ukraine War's Implications for Global Security: A First Multi-issue Analysis.* Geneva: Centre for Security Policy. Online: https://www.gcsp.ch/sites/default/files/2024-12/gcsp-analysis-russia-ukraine-war-implications.pdf

[78] Enkhardt 2023.

Haig Zsolt – Kovács László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* Budapest: Nemzeti Közszolgálati Egyetem. Online: https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf
Hofstetter, Yvonne (2020): *Láthatatlan háború, avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását.* Budapest: Corvina Kiadó.
Hybrid CoE [é. n.]: *What is Hybrid CoE?* Online: https://www.hybridcoe.fi/who-what-and-how/
Jójárt Krisztián (2020): A hibrid hadviselés és a jövő háborúja. *Honvédségi Szemle,* 148(1), 5–19. Online: https://doi.org/10.35926/HSZ.2020.1.1
Langerová, Erika (2025): China Holds a Kill Switch to European Power Grids. *Choice,* 2025. május 6. Online: https://chinaobservers.eu/china-holds-a-kill-switch-to-european-power-grids/
Lockheed Martin [é. n.]: *Golden Dome for America. Revolutionizing U.S. Homeland Missile Defense.* Online: https://www.lockheedmartin.com/en-us/capabilities/missile-defense/golden-dome-missile-defense.html
Ministry of National Defense of the People's Republic of China: Defense Policy. Online: http://eng.mod.gov.cn/2025xb/M/D_251593/
NATO (2007): Final Communiqué. Meeting of the North Atlantic Council in Defence Ministers Session. Online: https://www.nato.int/cps/en/natolive/news_47011.htm
NATO (2014): *Wales Summit Declaration.* https://www.nato.int/cps/en/natohq/official_texts_112964.htm
NATO (2019): *London Declaration.* Online: https://www.nato.int/cps/en/natohq/official_texts_171584.htm
NATO Defense College (2022): *How are Emerging and Disruptive Technologies Affect NATO's Core Tasks?* Rome: NATO Defense College. Online: https://bit.ly/4d5bE95
NATO (2022): *Strategic Concept.* Online: https://www.nato.int/content/dam/nato/web-ready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf
NATO (2024a): *Cyber Defence.* Online: https://www.nato.int/cps/en/natohq/topics_78170.htm
NATO (2024b): *Washington Summit Declaration.* Online: https://www.nato.int/cps/en/natohq/official_texts_227678.htm
NATO (2024c): *CWIX 2024: NATO's Largest-Ever Digital Interoperability Exercise Concludes.* Online: https://www.act.nato.int/article/cwix24-concludes/
NATO (2025a): *NATO Commercial Space Strategy.* Online: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-commercial-space-strategy
NATO (2025b): *The Hague Summit Declaration.* Online: https://www.nato.int/cps/en/natohq/official_texts_236705.htm
NATO (2025c): *Defence Innovation Accelerator for the North Atlantic (DIANA).* Online: https://www.nato.int/cps/en/natohq/topics_216199.htm
NATO Hybrid Threats and Hybrid Warfare Reference Curriculum 2024. Online: https://www.pfp-consortium.org/products/reference-curricula
NATO Science and Technology Organization (2025): *NATO Science and Technology Trends 2025–2045.* Online: https://sto-trends.com/

O'Connell, Jerome A. (1963): Radar and the U-Boat. *U.S: Naval Institute Proceedings,* 89(9). Online: https://www.usni.org/magazines/proceedings/1963/september/radar-and-u-boat

Paráda István (2018): A NATO kibervédelmi irányelveinek fejlődése. *Honvédségi Szemle,* 11(3), 3–13.

Peterson, Andrea (2017): Hackers Caused a Blackout for the First Time, Researchers Say. *The Washington Post,* 2016. január 5. Online: https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/

Porkoláb Imre – Hőnich Artúr (2021): A NATO útja a DIANA létrehozásáig és főbb fókuszterületei a védelmi innováció keretében. *Honvédségi Szemle,* 149(6), 20–35. Online: https://doi.org/10.35926/HSZ.2021.6.2

Porkoláb Imre – Hennel Sándor – Hegedűs Ernő (2023): A Védelmi Innovációs Kutatóintézet, a NATO DIANA és a hazai védelmi célú innováció új rendszere. *Haditechnika,* 57(5), 47–50. Online: https://real.mtak.hu/189783/1/HT_2023-5_cikk_10.pdf

Shahir, Mohammad Nazer – Boghairy, Ali (2024): Constructivist Analysis of Russia's Military Invasion of Ukraine (2022); Investigating Putin's Identity Model and Cognitive Actions. *Journal of World Sociopolitical Studies,* 8(4), 841–876. Online: https://doi.org/10.22059/wsps.2025.379457.1449

Szenes Zoltán – Siposné Kecskeméthy Klára (2019): *NATO 4.0 és Magyarország. 20 év tagság, 30 év együttműködés.* Budapest: Zrínyi Kiadó.

Szentgáli Gergely (2013): A NATO kibervédelmi politikájának fejlődése. *Nemzet és Biztonság,* 6(3–4), 76–83. Online: https://folyoirat.ludovika.hu/index.php/neb/article/view/4307/3516

The Alliance's Strategic Concept, 2010. Online: https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/strategic-concept-2010

United States National Security Strategy 2022. Online: https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

United States Space Force [é. n.]: *Space Threat Fact Sheet.* Online: https://www.spaceforce.mil/About-Us/Fact-Sheets/Fact-Sheet-Display/Article/4297159/space-threat-fact-sheet/

U.S. Department of State (1983): *Strategic Defense Initiative (SDI).* Online: https://2001-2009.state.gov/r/pa/ho/time/rd/104253.htm

Waterman, Shaun (2025): NATO Will Follow Space Force Lead with a Single Front Door for Industry. *Air and Space Forces Magazine,* 2025. július 29. Online: https://www.airandspaceforces.com/nato-space-force-front-door-industry/

World Bank Group [é. n.]: *GDP (constant 2015 US$) – China.* Online: https://data.worldbank.org/indicator/NY.GDP.MKTP.KD?end=2024&locations=CN&start=1961&view=chart