Molnár Dóra,✧ Nagy Gréta❖

# A 2023-as amerikai kiberbiztonsági stratégia áttekintése és értékelése

DOI 10.17047/Hadtud.2023.33.E.90

A 2023. március 2-án nyilvánosságra hozott új dokumentum, amely a Biden-Harris adminisztráció kibertérbeli politikájának alapjait rögzíti, a Trump-adminisztráció 2018-ban kiadott kiberbiztonsági stratégiáját váltotta fel. Az új stratégia sokban épít a korábbi dokumentumban foglaltakra, azonban több ponton egészen új megközelítést alkalmaz. E körben kiemelendő a kötelező érvényű szabályok szükségességének hangsúlyozása, a felelősségi körök megosztása a kiberszereplők között és Kína mint a legnagyobb fenyegetés említése a dokumentumban. A tanulmány előbb elemzi az új stratégia fő megállapításait, majd értékeli az Egyesült Államok új kiberbiztonsági célkitűzéseit, megvalósításuk esetleges korlátait. Az viszont biztosan állítható, hogy ha sikerül az új kiberstratégiában foglaltakat teljes mértékben végrehajtani, jelentősen javulhat az Egyesült Államok kiberbiztonsági helyzete.
Kulcsszavak: kiberbiztonság, Egyesült Államok, stratégia

## *Overview and assessment of the US Cybersecurity Strategy 2023*

*The Trump administration's 2018 cybersecurity strategy has been replaced by a new document, released on 2 March 2023, which sets out the basis for the Biden-Harris administration's cyberspace policy. The new strategy builds on much of the previous document, but takes an entirely new approach on several points. In particular, the document stresses the need for binding rules, the division of responsibilities between cyber actors and the mention of China as the biggest threat. The study first analyses the main findings of the new strategy and then assesses the new US cybersecurity objectives and the possible constraints to their implementation. However, it can be stated with certainty that if the new cyber strategy is fully implemented, the US cyber security posture could improve significantly.*
*Keywords: cybersecurity, United States, strategy*

### *1. Előzmények*

A kibertérről való stratégiai gondolkodás éppen 20 éves múltra tekint vissza, és megállapítható, hogy az Egyesült Államokban elnöki ciklusonként tipikusan egy, a kiberbiztonsággal kapcsolatos stratégiai dokumentum lát napvilágot.

Az első ilyen stratégia Bush elnök nevéhez köthető, aki 2003-ban kiadta első olyan nemzeti stratégiáját, amely a biztonságos kibertér megteremtését tűzte ki célul. A *Nemzeti Stratégia a Kibertér Védelmére* (National Strategy to Secure Cyberspace)[1] elnevezésű dokumentum a kiberbiztonságot a belbiztonság kritikus elemeként említi, és már ekkor különös hangsúllyal jeleníti meg a kritikus infrastruktúra védelmének fontosságát.

✧ adjunktus; Nemzeti Közszolgálati Egyetem (NKE), Hadtudományi és Honvédtisztképző Kar (HHK), Nemzetközi Biztonsági Tanulmányok Tanszék – *assistant professor; University of Public Service (UPS), Faculty of Military Sciences and Officer Training, International Security Policy Department;* e-mail: molnar.dora@uni-nke.hu, ORCID: 0000-0002-1476-5253
❖ Nemzeti Közszolgálati Egyetem, ÁNTK, Kiberbiztonsági mesterszakos hallgató, az ENISA kiberbiztonsági szakértője – *NUPS, Faculty of Public Governance and International Studies; Cybersecurity MA student, cybersecurity expert at ENISA;* email: gretanagyibs@gmail.com, ORCID: 0000-0001-5893-6985
[1] *National Strategy to Secure Cyberspace* 2003.

Az Obama-adminisztráció 2009-ben *A Kibertér-politika Felülvizsgálata* (Cyberspace Policy Review)[2] néven adta ki hivatalos stratégiáját, amely már felismerte, hogy a nemzet digitális infrastruktúrájának felépítése – amely nagyrészt az internetre épül – nem biztonságos és nem rugalmas, márpedig ez a védelem egyik kulcskérdése. Emellett rámutatatott két olyan kérdéskörre is, amelyek megoldása azóta valamennyi állam kiberagendájának napirendjén szerepel. Az egyik a felelősségi és hatáskörök nem megfelelő elhatárolása. A kiberbiztonsággal kapcsolatos felelősségi körök a szövetségi minisztériumok és ügynökségek széles skáláján oszlanak meg, gyakran egymást átfedő hatáskörökkel, és nincs olyan szervezet, amely elegendő döntési jogkörrel rendelkezne ahhoz, hogy a gyakran egymásnak ellentmondó kérdésekkel foglalkozó intézkedéseket következetesen irányítsa. A másik kérdéskör a köz- és magánszektor közötti megfelelő együttműködés és koordináció hiánya. Mivel az információs és kommunikációs hálózatok nagyrészt a magánszektor tulajdonában vannak és a magánszektor üzemelteti őket mind nemzeti, mind nemzetközi szinten, ezért a hálózatbiztonsági kérdések kezelése a köz- és a magánszféra partnerségét, valamint nemzetközi együttműködést és nemzetközileg elfogadott normákat igényel. Az Obama-adminisztráció azonban a liberális szellemiség jegyében már nem csak a nemzeti biztonsági kérdéseket helyezte előtérbe, hanem e speciális területen is nagy hangsúlyt fektetett a nemzetközi együttműködésre. Ennek megnyilvánulása volt az Egyesült Államok *Kiberterére vonatkozó nemzetközi stratégiájának* (International Strategy for Cyberspace)[3] elfogadása 2011-ben, amely akkor az amerikai kiberdiplomácia sarokkövét jelentette, és ezzel e specifikus terület az amerikai kül- és nemzetbiztonsági politika kritikus komponensévé vált.[4]

A Trump-adminisztráció 2018-ban adta ki az első stratégiáját, megalkotva első ízben az amerikai *Kiberbiztonsági stratégiát* (National Cyber Strategy).[5] Ezt megelőzően ilyen elnevezésű dokumentum nem létezett. A stratégia érdekessége az, hogy felépítése teljes mértékben követi a 2018-as amerikai Nemzeti biztonsági stratégia négypilléres felépítését. A dokumentum a kiberteret a lendületes digitális gazdaság motorjaként definiálja, és kiemeli, hogy ennek jövőbeli megtartásához szükség van a külföldi partnerekkel és más érdekelt csoportokkal, köztük a civil társadalommal és a magánszektor szereplőivel való intenzív együttműködésre. A stratégia több ponton is a Pentagon szerepét hangsúlyozza, továbbá kiemeli, hogy a tárca az amerikai fölény megőrzésére összpontosít a kibertérben, és előre védekezve (defense forward) megzavarja a rosszindulatú kiberszereplők tevékenységét, mielőtt azok elérnék az amerikai hálózatokat.[6]

Ezt a 2018-as dokumentumot váltotta fel az Egyesült Államok új Kiberbiztonsági stratégiája 2023. március 2-án.[7] Jelen tanulmányban arra vállalkozunk, hogy az új amerikai stratégia legfőbb elemeit bemutassuk és röviden értékeljük, továbbá rávilágítsunk arra, hogy ez az új stratégiai dokumentum mennyiben tekinthető a korábbi stratégiákban foglaltak továbbvitelének és mennyiben hoz újat, s ezáltal készül fel a jövő új kiberfenyegetéseire. A bevezető gondolatokat azzal zárjuk, hogy ezen átfogó, a kibertérre vonatkozó nemzeti stratégiák megalkotása mellett

[2] *Cyberspace Policy Review* 2009.
[3] *International Strategy for Cyberspace* 2011.
[4] Részletesebben lásd: Molnár 2022, 73–92.
[5] *National Cyber Strategy of the USA*, 2018.
[6] Cronk 2023.
[7] *National Cybersecurity Strategy*, 2023.

2011-től kezdve az Egyesült Államok Védelmi Minisztériuma különálló kiberstratégiát is kiad. Az első ilyen dokumentum 2011-ben született meg,[8] amelyet a 2015-ös,[9] majd a 2018-as[10] váltott fel.[11] (Az új dokumentum kiadása folyamatban van – e sorok írásakor a tervezetet a Minisztérium már megküldte a Kongresszusnak.) Ez azért is figyelemre méltó, mert összhangban áll azzal, az Egyesült Államok által már stratégiai szinten is a 2010-es évek elején felismert tendenciával, amely nem más, mint a kibertér militarizációja.

## *2. A stratégia ismertetése*

### *2.1. A régi-új stratégia*

Az Egyesült Államok 2023. évi kiberstratégiája a korábbi stratégiák szerves folytatásának tekinthető azzal, hogy számos újdonsággal is szolgál. Az előző három elnök által kiadott kiberbiztonsági stratégiákkal együtt olvasva az új dokumentum azt tükrözi, hogy a kibertámadás és a kibervédelem egyre inkább a nemzetbiztonsági politika központi elemévé vált.[12]

A Bush-kormányzat soha nem ismerte el nyilvánosan az amerikai kibertámadási képességeket, még akkor sem, amikor a legkifinomultabb kibertámadást intézte egy állam egy másik ellen: nevezetesen amikor az Egyesült Államok a Stuxnet segítségével sikeresen szabotálta az iráni nukleáris üzemanyag-előállító létesítmények működését. A későbbi években az Obama-kormányzat vonakodott megnevezni Oroszországot és Kínát, mint az amerikai kormányt ért nagyobb hackertámadások mögött álló hatalmakat, számára a kibertérbeli együttműködés propagálása volt az elsődleges. A Trump-kormányzat megerősítette a hackerek és az államilag támogatott külföldi szereplők elleni amerikai támadó kezdeményezéseket, és azzal kapcsolatban is riadót fújt, hogy a kínai távközlési óriáscég, a Huawei nagy sebességű 5G-hálózatokat építsen ki (elsősorban az Egyesült Államokban), attól tartva, hogy a vállalat ellenőrzése az ilyen hálózatok felett segítheti a kínai megfigyelést, vagy lehetővé teszi Peking számára, hogy konfliktus idején leállítsa a rendszereket. A Trump-kormányzat azonban nem fordított (kellő) figyelmet arra, hogy az amerikai vállalatoktól megkövetelje a kritikus infrastruktúrák minimális védelmének kialakítását és a cégeket felelősségre vonja a károkért, ha az általuk nem kezelt sebezhetőségeket kihasználják.

Az új stratégia sokban épít a korábbi dokumentumban foglaltakra,[13] azonban több ponton egészen új megközelítést alkalmaz. Ez utóbbi területen például egészen más alapokat fektet le mint az elődje, és a minimálisan elvárt kötelező standardek lefektetésének fontosságát hangsúlyozza a kritikus infrastruktúra számos szektorát érintően. Egy másik újdonság az, ahogyan szakít Obama

[8] *Department of Defense Strategy for Operating in Cyberspace*, 2011.
[9] *Department of Defense Cyber Strategy*, 2015.
[10] A Pentagon 2018-as kiberstratégiáját nem hozták nyilvánosságra; összefoglalása elérhető itt: Summary - Department of Defense Cyber Strategy 2018.
[11] A Pentagon új kiberstratégiájának megjelenése 2023-ban várható.
[12] Sanger 2023.
[13] Ez alatt értve nem csak a korábbi adminisztrációk hivatalos stratégiai kiberdokumentumait, hanem a következőket is: 14028. sz. elnöki rendelet (Improving the Nation's Cybersecurity - A nemzet kiberbiztonságának javítása), 5. sz. nemzetbiztonsági memorandum (NSM 5: Improving Cybersecurity for Critical Infrastructure Control Systems – A kritikus infrastruktúra-irányítási rendszerek kiberbiztonságának javítása), valamint az NSM 8 (Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems - A nemzetbiztonsági, védelmi minisztériumi (DoD) és hírszerzési közösségi rendszerek kiberbiztonságának javítása.

elnök „óvatos Kína politikájával” is, a kibertérben jelentkező legnagyobb fenyegetésnek nevezve az ázsiai országot. A továbbiakban ilyen és ehhez hasonló, az új kiberstratégiát jellemző vonásokra mutatunk rá részletesen.

### *2.2. A stratégia bemutatása*

Az új alapoknak lefektetését részben az elmúlt években elszenvedett olyan horderejű kibertámadások indokolták, amelyekre az Egyesült Államok nem volt felkészülve, ezért igen jelentős károkat tudtak okozni, részben pedig annak a gondolata, hogy a stratégia szerint az ország sorsdöntő évtized előtt áll, amikor a kiberteret érintően is alapvető változásokat kell végrehajtani, újra osztva többek között a szerepeket, a felelősséget és az erőforrásokat. (A változtatások végrehajtására a stratégia nem kevesebb, mint 65 milliárd dollárt különít el.) Az Egyesült Államok számára a kívánt végállapot egy olyan digitális ökoszisztéma kialakítása a szövetségesekkel és partnerekkel együtt, amely megvédhető, ellenálló és az alapvető értékeken nyugszik. Ez *kettős feladatot* ró az országra:

1. A kibertér védelmével kapcsolatos felelősséget újra kell egyensúlyozni azáltal, hogy a kiberbiztonsággal kapcsolatos terheket az egyénekről, a kisvállalkozásokról és a helyi önkormányzatokról azokra a szervezetekre kell hárítani, amelyek a legképzettebbek és a legjobb helyzetben vannak ahhoz, hogy csökkentsék a mindenki számára jelentkező kockázatokat.
2. Át kell alakítani az ösztönzőket, hogy a hosszú távú befektetéseknek kedvezzenek, és óvatos egyensúlyt kell teremteni a mai sürgős fenyegetések elleni védekezés, valamint az ellenálló jövő stratégiai tervezése és az abba való befektetés között.

A stratégia értelmében a kiberbiztonság olyan fundamentum, amely elengedhetetlen a következőkhöz: 1) a gazdaság alapvető működéséhez; 2) a kritikus infrastruktúra működéséhez; 3) az erős demokráciához és a demokratikus intézményekhez; 4) az adatok és a kommunikáció védelméhez; 5) a nemzeti védelemhez. Ezek elérése azonban elképzelhetetlen a köz- és magánszektor közötti szoros együttműködés és az olyan, hosszútávon megtérülő befektetések nélkül, amelyek az ország biztonságának, ellenállóképességének növelését és az új technológiák előtérbe kerülését ösztönzik. Hasonlóképpen fontos a szövetségesekkel és partnerekkel való még szorosabb együttműködés, hogy a felelős állami viselkedés szabályait megerősítsék és a felelőtlen állami viselkedésért az államokat felelősségre lehessen vonni. A cél annak biztosítása, hogy az internet hosszú távon is nyílt, szabad, együttműködő, megbízható és biztonságos maradjon. Az Egyesült Államok úgy érzi, hogy erős pozíciójából fakadóan készen áll ezen kérdések kezelésére, karöltve a kibertér más, szövetséges vezető hatalmaival.

A stratégia a bevezető részt követően öt tartalmi egységre bomlik, felvázolva ezzel a stratégia ötpilléres szerkezetét, amelyet végül egy végrehajtási záradék zár le.

***I.***

A *Bevezetés* szót ejt a technológiák pozitív és negatív hatásairól, egy klasszikus stratégiai környezetértékelést tartalmaz, nevesítve előbb az új tendenciákat, majd a rosszindulatú szereplőket. A stratégia szerint a négy fő új tendencia a következő:

- a szoftverek és a rendszerek egyre komplexebbé válása, amely a biztonság csökkenéséhez vezet – külön is nevesítve a mesterséges intelligenciával kapcsolatos aggályokat is;
- a felgyorsult globális konnektivitás, amely következtében egy rendszert ért támadás gyorsan átterjed más államok rendszereire is (mint például 2017-ben a NotPetya esetében);
- a digitális technológiák okozta kockázatok, amelyeket a koronavírus járvány miatti digitális átállás tovább erősített;
- a digitális és a fizikai világ közötti határ lebontásához vezet az összekapcsolhatóság új generációja. Számos gyár, erőmű még a régi analóg ellenőrzési rendszerekkel rendelkezik, amelyeket bár fokozatosan lecserélnek, az online technológiákra való áttéréssel azonban sérülékenyebbé is válnak.

A rosszindulatú szereplők között Kína, Oroszország, Irán és Észak-Korea kormányait nevesíti a stratégia, azzal, hogy más, revizionista szándékokkal rendelkező autokratikus államok is e körbe tartoznak. A stratégia ezen a ponton meglepően kemény szavakkal illeti a Kínai Népköztársaságot mint a legsúlyosabb, legaktívabb, legtartósabb fenyegetést: Kína az egyetlen ország, amelynek megvannak egyrészt a szándékai a nemzetközi rend megváltoztatására, másrészt a gazdasági, diplomáciai, katonai és technológiai képességei is a szándékai eléréséhez. Kína az elmúlt tíz évben rengeteget fejlődött, és mostanra képes lett az amerikai érdekeket fenyegetni és a fejlődő technológiákat uralni (amelyek a globális fejlődéshez elengedhetetlenek). Az Egyesült Államok szerint Oroszország – amely továbbra is tartós kiberfenyegetés marad – két évtizede arra használja a kiberkapacitásait, hogy destabilizálja a szomszédjait, és szerte a világban beavatkozzon a demokráciák belpolitikájába. Iránt és Észak-Koreát növekvő szofisztikáltság és a rosszindulatú tevékenységekre való akarat jellemzi: Irán arra használja a kiberképességeit, hogy az Egyesült Államok szövetségeseit a Közel-Keleten és szerte a világban fenyegesse, míg Észak-Korea célja a bevételnövelés a bűnözői szervezetek révén (kriptovaluta ellopása, zsarolóvírusok).

***II.***

A stratégia fő tartalmi részét az *öt pillér* tartalommal való megtöltése jelenti. A kiberstratégia öt pillére a következő:

1. A kritikus infrastruktúrák védelme.
2. A fenyegető szereplők megzavarása és felszámolása.
3. A piaci erők formálása a biztonság és ellenállóképesség növelése érdekében.
4. Befektetés a rugalmas jövőbe.
5. Nemzetközi partnerségek kialakítása a közös célok elérése érdekében.

### *1. A kritikus infrastruktúrák védelme:*

Ez a pillér öt részcélt nevesít, amelyek közül egyértelműen a leghangsúlyosabb a kiberbiztonsági kötelező követelmények felállítása, hiszen alapfeltétel, hogy a kritikus infrastruktúrák tulajdonosai és működtetői megfelelő kibervédelmet biztosítsanak. Olyan szabályozási környezetet kell kialakítani, amely igazodik a szektorok kockázati besorolásához, kerüli a duplikációkat, kiegészíti a köz- és magánszektor együttműködését, és összhangban áll a megvalósítás költségeivel. Az adminisztráció ilyen követelményeket már egyes szektorokat illetően megfogalmazott (például a kőolaj és földgáz vezetékek, a repülés, a vasút és a vízügyi rendszereket érintően), míg más szektorokban ez új hatóságok feladata lesz. A köz- és magánszféra együttműködésének kiszélesítése e területen is elengedhetetlen (e körben pozitív példaként szolgál a „Shield Up" kampány). A stratégia megjegyzi, hogy bár a magánszektor az esetek többségében képes közvetlen szövetségi segítség nélkül kezelni az incidenseket, de a vállalatoknak tudniuk kell, hogy mely kormányzati ügynökséget milyen célból kereshetnek fel, ha szükségessé válik. A Kiberbiztonsági Felülvizsgáló Bizottság (Cyber Safety Review Board - CSRB) célja, hogy összehozza a köz- és magánszféra kiberbiztonsági vezetőit, törvénymódosítás segítségével pedig a testületet a Belbiztonsági Minisztérium alá kívánják rendelni. Szükséges továbbá új és innovatív kapacitások kiépítése, hogy az együttműködés még hatékonyabb és még nagyobb volumenű legyen a kritikus infrastruktúra részvevő szervezeti között. A szövetségi ügynökségeknek növelniük kell a saját képességeiket, és incidens esetén a szövetségi szintű választ össze kell hangolni a magánszektorral és az ún. SLTT (State, local, Tribal, territorial) partnerekkel. Ez utóbbi kifejezés – amely többször is előfordul a dokumentumban – összefoglaló elnevezése az amerikai kiberbiztonság megteremtésében részt vevő közszereplőknek, azaz az államot, a helyi szervezeteket, a törzsi szervezeteket és a területi szerveket foglalja magában.

### *2. A fenyegető szereplők megzavarása és felszámolása:*

E célból az USA kész alkalmazni a nemzeti hatalom valamennyi eszközét, integrálva a diplomáciai, információs, katonai (kinetikus és kiber), pénzügyi, titkosszolgálati és rendőri kapacitásokat. Ehhez integrálni kell a szövetségi zavarelhárítási tevékenységeket (amelyben az Igazságügyi és a Védelmi tárcának van elsődleges szerepe), javítani kell a hírszerzési információk megosztásán, és e körben is szükséges a köz- és magánszektor műveleti együttműködésének erősítése. Az Egyesült Államok kiemelt figyelmet fog fordítani a kiberbűnözés elleni küzdelemre, azon belül is a zsarolóprogramok legyőzésére, amely politikáját négy elemre építi: 1) a nemzetközi együttműködés fokozása; 2) a zsarolóvírussal megvalósított bűncselekmények nyomozása, kivizsgálása, rendőri és más hatóságok segítségével; 3) a kritikus infrastruktúra ellenállóképességének növelése, valamint 4) a virtuális valutával való visszaélés kezelése a váltságdíjfizetések tisztára mosása érdekében. Ennek érdekében előbb a Fehérház indított útjára egy kezdeményezést több, mint 30 állam részvételével,[14] majd 2023 januárjában egy munkacsoportot is felállítottak Ausztrália vezetésével, valamint nemzeti szinten a CISA és az FBI elnökletével működik a Közös zsarolóvírus munkacsoport (Joint Ransomware Task Force - JRTF).

### *3. A piaci erők formálása a biztonság és ellenálló képesség növelése érdekében:*

[14] Counter-Ransomware Initiative (CRI).

A cél az olyan digitális gazdaság, amelyben a felelősséget arra hárítják, akik a kockázatok csökkentéséhez a lehető legjobb pozícióban vannak. Ez a megközelítés merőben új, hiszen a felelősség ezáltal átkerül a végfelhasználókról azokra, akik valóban képesek lépéseket tenni az incidensek bekövetkezése ellen. Ez pedig a piacot arra fogja ösztönözni, hogy biztonságosabb termékeket és szolgáltatásokat állítsanak elő. Ezáltal előmozdítható a magánélet védelme és a személyes adatok biztonsága, valamint a szövetségi támogatási programok elősegíthetik a biztonságos és ellenálló új infrastruktúrába történő beruházásokat is. A stratégia az adatvédelmet elsősorban az adatkezelők elszámoltathatóságával látja megvalósíthatónak, amelyhez törvényhozási lépések és nemzeti előírások megalkotása szükséges, külön kiemelve az olyan érzékeny adatok védelmét, mint az egészségügyi adatok és a geolokációs adatok. Az adatvédelem mellett elengedhetetlen a biztonságos IoT-eszközök fejlesztésének ösztönzése, amelyben kiemelt szerepe van a szövetségi kutatás-fejlesztésnek, cél továbbá egy IoT biztonsági címkézési rendszer életre hívása, amelyet a különböző IoT-termékekre lehetne alkalmazni, és amely a fogyasztóknak némi képet adna arról, hogy a termékek mennyire biztonságosak. Továbbra sem világos azonban, hogy ezek a címkék hogyan vonatkozhatnak az Egyesült Államokon kívüli vállalatok által gyártott termékekre.[15]

Az ösztönzők pénzügyi alapjait már korábban lefektették, elsősorban a Kétpárti infrastrukturális törvénnyel (Bipartisan Infrastructure Law), az Inflációcsökkentési törvénnyel (Inflation Reduction Act), valamint az ún. Chip törvénnyel (CHIPS and Science Act).

### *4. Befektetés a rugalmas jövőbe:*

Egy ellenálló és virágzó digitális jövő a ma megtett befektetésekkel kezdődik, amelyek révén az Egyesült Államok továbbra is világelső lesz a biztonságos és rugalmas, következő generációs technológiák és infrastruktúrák innovációjában, kiberbiztonsági K+F prioritásként kezelve a következő generációs technológiákat (számítógépes technológiák, a biotechnológia és a tiszta energia technológiák). Ugyanakkor fel kell készülni a kvantumtechnológia utáni jövőre is, amelyhez a ma egyik legégetőbb problémáját, a kibermunkaerő hiánya leküzdésének kérdését is meg kell oldani. Jelenleg az Egyesült Államokban 100.000 betöltetlen kiber munkahely van, és ez a szám egyre csak nő. Elsődleges cél a merítési alap szélesítése, mivel a nők, színes bőrűek, elsőgenerációs értelmiségiek, bevándorlók, fogyatékkal élők igen alulreprezentáltak ezen a területen. Ez a probléma érinti a fegyveres erőket is, ezért nem véletlen, hogy a stratégia kiadását megelőző napon, 2023. március 1-jént megjelent a Védelmi Minisztérium Kibermunkaerő stratégiája, amely a védelmi szektor kiber munkaerővel való ellátási problémájának megoldási kereteit vázolja fel 2027-ig.[16]

### *5. Nemzetközi partnerségek kialakítása a közös célok elérése érdekében:*

[15] *Highlights from the New U.S. Cybersecurity Strategy*. 2023.
[16] *DoD Cyber Workforce Strategy 2023-2027.*

Az Egyesült Államok évtizedek óta dolgozik nemzetközi szervezetekben (kiemelten az ENSZ Kormányzati Szakértő Csoportjában[17]) azon, hogy a felelős állami magatartásszabályokat megalkossák, de a nemzetközi együttműködés segítésére már számos egyéb mechanizmus is rendelkezésre áll. 2022 áprilisában az Egyesült Államok kiadta az internet jövőjéről szóló nyilatkozatot (Declaration for the Future of the Internet - DFI), amelyhez már több, mint 60 állam csatlakozott, emellett az egész világot lefedő partnerségi hálóval rendelkezik.[18] A cél a kibertérben, hogy a felelős állami magatartás legyen az alapvető elvárás, míg a felelőtlen magatartást a nemzetközi koalíciók és a hasonlóan gondolkodó nemzetek közötti partnerségek révén elszigeteljék és költségessé tegyék.

***III.***

Ami a stratégia *végrehajtásáról* szóló záró részt illeti, a végrehajtás koordinálásáért az a Nemzeti Kibervédelmi Igazgató Hivatala felel (Office of National Cyber Director – ONCD), amely vezetője, Chris Inglis 2023. február 15-én mondott le, köztudottan azt követően, hogy az új stratégiát már eddigre megalkották. A végrehajtás során az egyik fontos szempont a hatékonyság értékelése, amelyet a szövetségi kormány adatalapú megközelítésével az ONCD végzi el, és évente jelent az amerikai elnöknek, az elnök nemzetbiztonsági tanácsadójának és a kongresszusnak. Fontos továbbá a levont tanulságok állandó jellegű beépítése a végrehajtási folyamatba, valamint a kiberbiztonsági kiadások prioritásainak folyamatos felülvizsgálata.

### *3. A stratégia értékelése*

Elsőként a stratégia hatályát emeljük ki, amely a kiberbiztonságra korlátozódik – ezt türközi már a stratégia címe is, hiszen a dokumentum a „Nemzeti kiberbiztonsági stratégia” címet viseli és nem „Nemzeti kiberstratégia”. A stratégia közzétételéről szóló számos sajtójelentésben a kettőt összemossák, de hatályukat tekintve ezek nem azonosak. Az amerikai kormányzat általában a „kiberbiztonság” az NSPD-54 (és a HSPD-23) alapján 2008-ban kihirdetett definíciója alapján működik, amelynek érdekessége egyrészt az információs vagy befolyásolási műveletekre való utalás hiánya, másrészt a kibertérben végrehajtott támadó műveleteknek a szerteágazó nemzeti célok előmozdítására való felhasználása.[19] Ha a Biden-adminisztráció kiberstratégiát alkotott volna, ezek a kérdések mindenképpen szerepeltek volna benne.[20]

[17] UN Group of Governmental Experts

[18] Ilyenek többek között a Négyoldalú biztonsági párbeszéd (Quadrilateral Security Dialogue - „the Quad”) az Egyesült Államok, India, Japán és Ausztrália részvételével, az Indo-csendes-óceáni gazdasági keret a jólétért (Indo-Pacific Economic Framework for Prosperity - IPEF), az Amerikai partnerség a gazdasági megfelelőségért (Americas Partnership for Economic Properity - APEP), az AUKUS az Egyesült Államok, az Egyesült Királyság és Ausztrália részvételével, valamint az USA-EU Kereskedelmi és Technológiai Tanács (U.S.-EU Trade and Technology Council - TTC).

[19] National Security Presidential Directive -54 (Homeland Security Presidential Directive-23), azaz az 54. sz. elnöki nemzetbiztonsági rendelet (amely egyben a 23. sz. belbiztonsági elnöki rendelet), amely értelmében a kiberbiztonság a számítógépek, elektronikus hírközlési rendszerek, elektronikus hírközlési szolgáltatások, vezetékes hírközlés és elektronikus hírközlés – beleértve az azokban foglalt információkat is – károsodásának megelőzése, védelme és helyreállítása a számítógépek rendelkezésre állásának, integritásának, hitelesítésének, bizalmas jellegének és visszautasíthatatlanságának biztosítása érdekében.

[20] Lin 2023.

Az alábbi kérdések azok, amelyeket illetően jelen stratégia a korábbi három adminisztráció kiberbiztonsági erőfeszítéseitől gyökeresen eltér:

1. *A kiberbiztonsági terhek újbóli kiegyensúlyozása*: A stratégia értelmében az Egyesült Államok immáron nem, illetve nem csak a végfelhasználóktól várja el a kiberbiztonságuk garantálását, a felelősség terén a kormányzatnak és a magánszektornak is hatványozottan nő a szerepe. Ez utóbbi egyébiránt igen hangsúlyosan jelenik meg a dokumentumban, olyan összefüggésben is, hogy a köz- és magánszféra együttműködésére még fokozottabban szükség van.

2. *Szabályozás*: A stratégia egyik legjelentősebb újítását a szabályozás új alapokra helyezése jelenti. A magánszektor kiberbiztonságának ösztönzésére irányuló hagyományos, az önkéntes köz- és magánszféra közötti partnerségekre és információmegosztási gyakorlatokra összpontosító megközelítés helyett a stratégia megjegyzi, hogy bár az ilyen megközelítés néha javította a magánszektor kiberbiztonsági helyzetét, az ilyen javulások összességében nem voltak elegendőek a kiberbiztonsággal kapcsolatos nemzeti igények kielégítéséhez. A kiberbiztonság megvalósítását nem lehet egyszerűen az egyes magánszektorbeli szereplőkre bízni, akik kizárólag saját üzleti igényeik alapján döntenek. Ezért a stratégia agresszívebb és átfogóbb szövetségi szintű kiberbiztonsági szabályozást szorgalmaz, szükséges minimálisan elvárt kiberbiztonsági gyakorlatok vagy eredmények kötelező jelleggel történő meghatározásával – ami nem meglepően az érintett szereplők ellenállásába fog ütközni. Mivel azonban a képviselőházat jelenleg a republikánusok irányítják, a kormányzatnak kemény harcot kell majd vívnia e jogszabályi változtatásokért.[21] Külön probléma, hogy a szövetségi kormánynak nincs lehetősége arra, hogy kiberbiztonsági követelményeket támasszon az olyan állami intézményekkel szemben, mint például a kórházak, amelyek a hackerek „kedvelt”célpontjai”.[22]

3. *Felelősség* a nem biztonságos szoftvertermékekért és szolgáltatásokért: A stratégia kifejezetten elismeri, hogy a szoftverpiac túlságosan gyakran jutalmazza a biztonságba nem kellőképpen beruházó eladókat nagyobb piaci részesedéssel és a piacra kerülési idő csökkenésével. S bár számos kiberbiztonsági elemző évek óta támogatja a felelősségvállalást, amely arra ösztönzi a forgalmazókat, hogy nagyobb figyelmet fordítsanak a kiberbiztonságra, most először kerül erre sor stratégiai szinten is egy, a végrehajtó hatalom teljes támogatását élvező dokumentumban.

   A felelősségnek az iparra való áthárítását célzó jogszabályok megalkotása hosszú távú, akár egy évtizedes folyamat is lehet. Ráadásul várhatóan nem csak a nagy technológiai iparágak, hanem az Amerikai Kereskedelmi Kamara is ellenállást tanúsít majd, amely korábban a biztonsági előírások kötelezővé tétele ellen lobbizott.

   A felelősséggel kapcsolatban a stratégia olyan védett „helyeket” javasol, amelyek megóvják a vállalatokat a felelősségtől, ha biztonságosan fejlesztik és karbantartják szoftvertermékeiket és szolgáltatásaikat. Az ilyen felelősség jellegének, hatályának és

[21] Widakuswara 2023.
[22] Sanger 2023.

mértékének meghatározása azonban még hátra van, és olyan kérdésekre is választ kell majd adni, mint: Milyen bizonyítékokat kell figyelembe venni a felelősség mértékének enyhítéseként? Hogyan kell felosztani a felelősséget a több fél tevékenységéből eredő kiberbiztonsági jogsértésekért? Meg kell-e szabni a felelősség felső határát bizonyos szinteken, és ha igen, milyen alapon? Mi a biztosítók szerepe a szoftverfelelősség világában? Be kellene-e tiltani a csoportos kereseteket? Természetesen számos további hasonló kérdés vár még megválaszolásra.

A kormányzat továbbá biztosítani szeretné, hogy a biztosítótársaságok megfelelő finanszírozással rendelkezzenek a jelentős vagy katasztrofális kiberbiztonsági incidenseket követő kárigényekre való reagáláshoz. 2020 óta a kiberbiztonsággal kapcsolatos biztosítások piaca közel 75%-kal nőtt, és valamennyi szervezet (méretétől függetlenül) szükségesnek tartja az ilyen biztosításokat. Ez érthető, tekintve, hogy számos vállalat és kormányzati szerv a napi működés során az internetre és a vállalati hálózatokra támaszkodik. A kormányzat a kiberbiztonsági biztosítók védelmétől, vagyis a „backstoppingtól" azt reméli, hogy egy kiberbiztonsági incidens során a biztosítók és az áldozatok számára megelőzhető egy jelentős rendszerszintű pénzügyi válság.[23]

4. A *fenyegető szereplők* megzavarása és felszámolása: A stratégia a már említett rendkívül határozott megközelítés mellett nem zárkózik el a *katonai erő alkalmazásától* sem az ilyen jellegű zavarás érdekében, amennyiben az helyénvaló. Ez utóbbi egyébiránt már most is nyilvánvaló, elnézve az amerikai kiberparancsnokság által a külföldi zsarolóvírus-szereplők tevékenységének megzavarása érdekében végrehajtott offenzív kiberműveleteit. Külön érdekessége a stratégiának, hogy a zsarolóvírusok jelentette fenyegetésre mint az Egyesült Államokat a kormányzat és az üzleti élet minden szintjén fenyegető legégetőbb fenyegetésre tekint, és a zsarolóvírus-fenyegetéseket már nem bűnügyi tevékenységként, hanem nemzetbiztonsági problémaként kezeli.

   A Védelmi minisztérium és a hírszerző közösség hatékony védelmi erőfeszítései elkerülhetetlenül szorosabb kapcsolatokat fognak jelenteni a nemzetbiztonsági hatóságok és a polgári infrastrukturális eszközök tulajdonosai és üzemeltetői között. Példának okáért a polgári eszközök széles körét érintő hatékony támadásértékelés szükségessége technikai, jogi és politikai koordinációt igényel a magánszektor és az amerikai kormányzat között. Ez – egyebek mellett – jelentős védelmi minisztériumi jelenlétet vonhat maga után a magántulajdonban lévő hálózatokon – hogy az amerikaiak hogyan reagálnak majd minderre, még a jövő zenéje.

Végezetül a stratégiával kapcsolatban két problémás területet nevesítünk. A stratégia ígéretet tesz a szövetségi minősítési politika felülvizsgálatára annak megállapítására, hogy hol van szükség további minősített információkhoz való hozzáférésre – a valóság azonban az, hogy már most is problémás a túlzott titkosítás, gyakran képezi az együttműködés gátját. A stratégia másik hiányossága, hogy nem foglalkozik a kibertaktikák, -technikák és -eljárások felhasználásával a befolyásolási vagy dezinformációs kampányokban és más, az Egyesült Államokat célzó akciókban. Elképzelhető, hogy ez a kihagyás szándékos, mert bár a kiberbiztonság és a

[23] Rundle 2023.

befolyásolási műveletek gyakran összefonódnak, a befolyásolási műveletek elleni küzdelemre való hivatkozás pártpolitikai konfliktusokhoz vezethet a szólásszabadsággal és a politikai tevékenységgel kapcsolatban. Ugyanakkor a stratégia előremutató megállapítása, hogy az Egyesült Államok elkötelezett az amerikai űrrendszerek védelme és ellenállóképessége növelés iránt, beleértve Az űrrendszerek kiberbiztonsági alapelvei (Space Policy Directive 5 - Cybersecurity Principles for Space Systems) c. hivatalos dokumentum végrehajtását is – tegyük hozzá, hogy nem hiába, hiszen már mindenki számára nyilvánvaló, hogy az űr és a kibertér egymástól elválaszthatatlan közös terek, ahol könnyen elképzelhető, hogy a jövő háborúit fogják vívni. De ne szaladjunk ennyire előre. Ami viszont biztos, az az, hogy ha sikerül az új kiberstratégiában foglaltakat teljes mértékben végrehajtani, jelentősen javulhat az Egyesült Államok kiberbiztonsági helyzete.

### *4. Összegző gondolatok*

A 2023-as nemzeti kiberbiztonsági stratégia egyértelműen az Egyesült Államok azon törekvésének az eredménye, hogy továbbra is alakítsa a globális kibertér jövőjét, amely – az egyre növekvő kínai jelenlét ellenére is – nagymértékben függ az amerikai infrastruktúrától. A kiemelt témák és célkitűzések összhangban vannak azzal, ahogyan Washington a globális technológiai szétválásban navigál, és minden bizonnyal támogatni fogják az Egyesült Államok gazdasági ellenálló képességét és kiberbiztonságát a többpólusú globális rendezetlenség korában.

A jövőre nézve a stratégia sikeres végrehajtása fogja meghatározni az amerikai kibertér biztonságát és ellenálló képességét, valamint a tágabb értelemben vett dinamikát, hiszen egyik oldalról a szövetségesek követni fogják az amerikai példát, míg a másik oldalról az ellenfelek kibereszközökkel próbálják majd továbbra is fenyegetni az Egyesült Államok biztonságát. Az, hogy a stratégia milyen mértékben eredményezheti a kívánt inkluzív szabályozás megalkotását, attól függ, hogy a törvényhozók és a magánszektor milyen gyorsan és hatékonyan tud összehangolódni a Biden-kormányzat megközelítésének alapelveivel. Tekintettel arra, hogy a magánszektorbeli szervezetek milyen sokféleképpen érintettek a stratégiában és a javasolt politikai megközelítésekben, ez a legtöbb területen igen összetett és nehéz feladatnak ígérkezik. Az mindenesetre érdekes lesz majd látni, hogy az adminisztráció mikor melyik kart fogja megmozgatni, hogy a stratégia vízióját előrevigye.

## FELHASZNÁLT IRODALOM

*A Pentagon 2018-as kiberstratégiájának hivatalos összefoglalása*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF Letöltés ideje: 2023. március 30.

Cronk, Terri Moon 2023: *White House Releases First National Cyber Strategy in 15 Years.* https://www.jcs.mil/Media/News/News-Display/Article/1643010/white-house-releases-first-national-cyber-strategy-in-15-years/ Letöltés ideje: 2023. március 30.

*Cyberspace Policy Review* 2009, https://obamawhitehouse.archives.gov/cyberreview/documents/, https://irp.fas.org/eprint/cyber-review.pdf Letöltés ideje: 2023. március 30.

*Department of Defense Strategy for Operating in Cyberspace*, 2011. július, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf Letöltés ideje: 2023. március 30.

*Department of Defense Cyber Strategy*, 2015. április file:///D:/molnard/Downloads/764848.pdf (Letöltés ideje: 2023. március 30.)

*DoD Cyber Workforce Strategy 2023-2027,* https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf Letöltés ideje: 2023. május 30.

*Highlights from the New U.S. Cybersecurity Strategy*. 2023. március 2. https://krebsonsecurity.com/2023/03/highlights-from-the-new-u-s-cybersecurity-strategy/ Letöltés ideje: 2023. március 30.

*International Strategy for Cyberspace* 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf Letöltés ideje: 2023. március 30.

Lin, Herb: *Where the New National Cybersecurity Strategy Differs From Past Practice*. 2023. március 6. https://www.lawfareblog.com/where-new-national-cybersecurity-strategy-differs-past-practice Letöltés ideje: 2023. március 30.

Molnár Dóra: Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi porondon. In: *Kiberdiplomácia* (szerk.: Molnár Anna – Molnár Dóra). Ludovika Egyetemi Kiadó, Budapest, 2022, 73–92.

*National Cyber Strategy of the USA,* 2018. szeptember, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf Letöltés ideje: 2023. március 30.

*National Cybersecurity Strategy,* 2023. március, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf Letöltés ideje: 2023. március 30.

*National Security Presidential Directive -54* (Homeland Security Presidential Directive-23) – 54. sz. elnöki nemzetbiztonsági rendelet (egyben a 23. sz. belbiztonsági elnöki rendelet). 2008. január 8., https://irp.fas.org/offdocs/nspd/nspd-54.pdf

*National Strategy to Secure Cyberspace* 2003, https://georgewbush-whitehouse.archives.gov/pcipb/ Letöltés ideje: 2023. március 30.

Rundle, James: *U.S. Government to Explore Cyber Insurance Backstop.* 2023. március 6. https://www.wsj.com/articles/u-s-government-to-explore-cyber-insurance-backstop-ddc94c11 Letöltés ideje: 2023. május 30.

Sanger, David E.: *New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms.* 2023. március 2. https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html Letöltés ideje: 2023. március 30.

*Summary - Department of Defense Cyber Strategy 2018*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF Letöltés ideje: 2023. március 30.

Widakuswara, Patsy: *US Launches Aggressive National Cybersecurity Strategy*. 2023. március 2. https://www.voanews.com/a/us-launches-aggressive-national-cybersecurity-strategy-/6986279.html Letöltés ideje: 2023. március 30.