Szemelvények a katonai műszaki tudományok eredményeiből II.

Hallgatói kötet

Szerkesztette
Hausner Gábor

LUDOVIKA
EGYETEMI KIADÓ

Szemelvények a katonai műszaki tudományok eredményeiből II.

Szemelvények a katonai műszaki tudományok eredményeiből II.

Hallgatói kötet

Szerkesztette

Hausner Gábor

LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2021

Szerzők

Ambrus Éva
Bodnár László
Csanádi Győző
Deák Veronika
Dévai Dóra
Domán László
Goda Zoltán
Huszár Péter
Huszár Viktor
Katona Gábor
Kralovánszky Kristóf
Kretz András
Kutassy Emese
Lakatos Bence Roland
Matusz Márk Péter
Olajosné Lakatos Boglárka
Priváczkiné Hajdu Zsuzsanna
Salamon Endre
Takács Krisztina
Terék Tamás
Tímár Attila

Szakmai lektorok

Bíró Tibor
Haig Zsolt
Padányi József
Palik Mátyás
Pohl Árpád
Restás Ágoston

Ludovika Egyetemi Kiadó
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu
A kiadásért felel: Koltay András rektor
Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Oláh Andrea
Korrektor: Bíró Csilla, Bujdosó Hajnalka
Tördelőszerkesztő: Fehér Angéla

ISBN 978-963-531-441-6 (PDF) | ISBN 978-963-531-442-3 (ePub)

Tartalom

Huszár Viktor

A blokklánc, a számítógépes látás és a mesterséges intelligencia alkalmazási lehetőségei a kiberhadviselésben

Bevezetés

Magyarország 2020-ban kiadott Nemzeti Biztonsági Stratégiája bevezetőjében így fogalmaz: „A hazai védelmi ipar, azon belül is a kutatás-fejlesztés és az innováció támogatása nemzetbiztonsági érdek, mivel ezek által csökkenthető az import függőség, növelhető az ellátásbiztonság és hazai gyártmányokkal korszerűsíthetőek a védelmi eszközök."[1] A gépi látás és a hozzá kapcsolódó mesterségesintelligencia-kutatások a védelmi szektorban kiemelt fontosságúak, a legfejlettebb technológiával rendelkező országok széles körben használják, ám a magyar rend- és honvédelmi környezetben ezen megoldások használata kezdetleges. A gépi látásra alapuló mesterséges intelligencia felhasználási területe katonai műszaki tudományos kihívások sokaságát veti fel. Azonban az elmúlt néhány évtized megmutatta, amit már tudtunk – az információtechnológia nemcsak fejlődik, de számos iparágat is felborít azzal, hogy a növekedés és a fejlődés terén egyedülálló lehetőségeket kínál. A következő generációs technológiák, a gépi tanulás és a mesterséges intelligencia megadja a lehetőséget a katonaságnak és a rendvédelmi erőknek az átalakuláshoz, és hogy továbbra is megőrizhessék saját ágazatukat.

Az Amerikai Egyesült Államok már az 1990-es években is alkalmazott digitális technológiát, például hálózatközpontú műveleteket, amelyek ötvözték azokat a „taktikákat, technológiákat és eljárásokat, amelyeket egy hálózattal ellátott haderő arra alkalmazhat, hogy döntő harctéri előnyre tegyen szert".[2] 1995-ben Bower és Christensen reflektorfénybe állította a „diszruptív technológiákat", amelyek segítségével a versenytársak a verseny élén maradhatnak. Kutatásuk megmutatta, hogy a jó alapokkal rendelkező vállalatok többségének eltökélt szándéka, hogy iparáguk előtt járjanak az „új technológiák fejlesztésének és piaci alkalmazásának" területén, és ez a lépésről lépésre történő fejlesztésektől az egészen progresszív, teljes iparágakat átformáló megközelítésekig terjedhet – amelynek fő célja, hogy az ilyen fejlesztések az „ügyfeleik következő generációs szükségleteit célozzák".[3] Nagyjából ezzel egyidőben jelent meg egy mindent átszövő

---

[1] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

[2] John J. Garstka: Network-centric warfare offers warfighting advantage. *Afcea.org,* May 2003.

[3] Joseph L. Bower – Clayton M. Christensen: Disruptive technologies: Catching the wave. *Harvard Business Review,* (1995), 1–2.

információs hálózat, amely a blokklánc-technológián alapul – egy olyan technológián, amely képes arra, hogy központi irányítás nélkül tároljon el biztonságosan, módosítást kizáró módon adatokat.[4]

Ugorjunk előre pár évtizedet, és láthatjuk, hogy a Distributed Ledger Technology (elosztott főkönyvi technológia) nagy hatással van számos ágazatra, nagyban befolyásol gazdasági rendszereket, jogi kereteket és információs technológiákat.[5] Érdemes megjegyezni, hogy amíg a kereskedelmi iparágak mindent megtettek, hogy előnyre tegyenek szert a blokklánc-technológia terén, és bizonyos fokú vizsgálatnak vetették alá a szabályozás hiányosságait, addig sokkal kevesebb figyelmet fordítottak a blokklánc-technológiában rejlő lehetőségekre és annak sebezhetőségére a katonai hírszerzés és a rendvédelem terén. A következő alfejezetek nagy vonalakban meghatározzák a blokklánc-technológiát, hogy előrevetítsék a lehetséges kapcsolatokat a technológiák között, a katonai hírszerzés és a rendvédelem szektorában való alkalmazási lehetőségek szempontjából. A védelmi igazgatásban ugyanis jelentős kihívást jelent, hogy a nagy mennyiségű, elosztott és különböző hálózatokból származtatható információkat miként lehet biztonságosan összegyűjteni, elemezni, és időzített döntéshozatalra előkészíteni.

A blokklánc-technológia meghatározása

A blokklánc egy elosztott adattárolási megoldás, ahol a „blokklánc" olyan adatklaszterek (adatblokkok) listáját jelenti, amelyek korlátok nélküli láncba rendeződve elosztott adatbázist hoznak létre. Minden blokk kapcsolódik az előző blokkhoz minden csomóponton (résztvevő), ami a blokkláncot tárolja. A blokkláncrendszerek alapvető jellemzője a blokkláncccsomópontok tárolása sorba rendezett feljegyzésekben, egységes megegyezéssel az aktuális állapotról, *konszenzusalapú* megközelítés szerint. Bár az elosztott adattárolásnak ezt a megközelítését a Bitcoin elosztott „kriptovaluta" keretrendszere tette népszerűvé, jelenleg számos alternatív rendszer is létezik, illetve áll fejlesztés alatt, amelyek ugyanezt az elvet követik, de céljaikban és a kulcsfontosságú technológiájuk terén alapvetően eltérnek. A jelenlegi helyzet szerint ezeket a rendszereket összefoglalóan és helytelenül egységesen „blokklánc-technológiának" nevezik.

A blokklánc képességei közé tartozik, hogy decentralizálja a tranzakciókat, miközben megnöveli a biztonságot, ezért fektettek a technológiai vállalatok abba, ami valószínűleg a következő technológiai forradalmat jelenti és nagy hatással lesz a társadalmi és gazdasági átalakulásban és az internet formálásában.[6] A blokklánc elosztott hibatűrésének

[4] Stuart Haber – W. Scott Stornetta: How to time-stamp a digital document. *Journal of Cryptology,* 3. (1991), 2. 99–111.

[5] Jesper Carvalho Andersen: The great chain of being sure about things. *The Economist,* October 31, 2015.

[6] Don Tapscott – Alex Tapscott: *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the worlsd.* New York, Portfolio/Penguin, 2016.

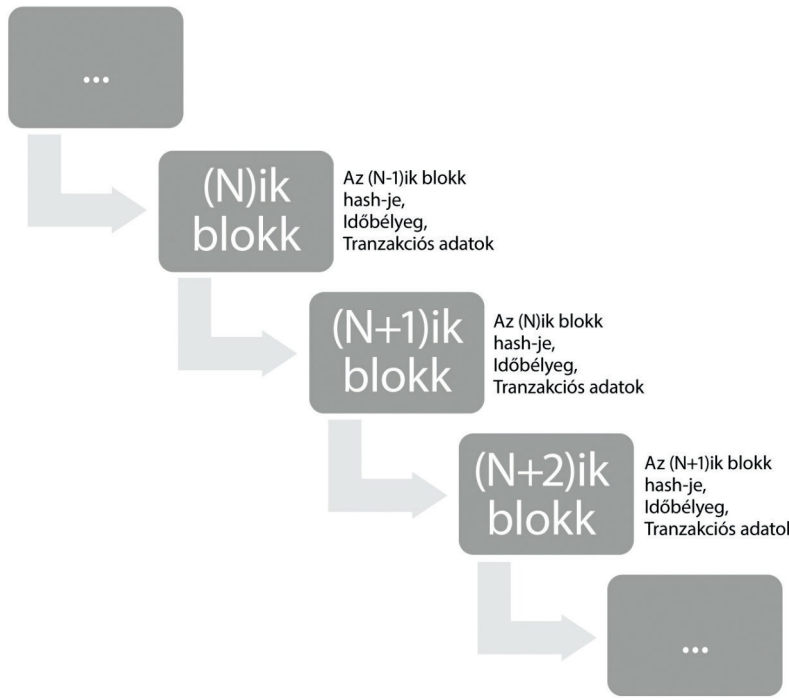
és zökkenőmentes tranzakcióinak fontosságát felismerte a katonai szektor, és már folynak kutatások arra nézve, hogy a meglévő rendszereket át lehet-e teljes egészében vagy részben állítani blokkláncalapúra.

A blokklánc-technológiák elosztott főkönyvet alkalmaznak és bővítik azt az elosztott hálózat csomópontjainak folyamatos szinkronizálása során. A hálózat elemei térben egymástól távol is lehetnek, vagy más vállalat tulajdonában is állhatnak, így a hálózatnak a főkönyvről minden csomóponton van másolata. A főkönyv minden kiegészítését jóvá kell hagynia más csomópontoknak is, ezt követően pedig a jóváhagyott blokk perceken vagy akár másodperceken belül megjelenik a többi csomóponton, a használt megoldás függvényében. Az eltárolt feljegyzésekhez bármelyik megbízható, központi ellenőrző szerv hozzáfér anélkül, hogy az érintené az adott szervezet saját belső eljárásait és szabályait.[7]

A főkönyvet az elosztott hálózat csomópontjai tartják fenn számos konszenzus algoritmus alapján, a tranzakciók tárolására és jóváhagyására kriptográfiát alkalmazva. Ezzel lehetővé válik, hogy a hálózat akkor is működőképes maradjon, ha nagy számban fordulnak elő hibás csomópontok, ameddig a hibás csomópontok száma nem haladja meg a megengedett maximumot. A blokkláncnak van egy általános szerkezete, amelyre tranzakciós naplóként *(log)* is tekinthetünk, amelynek az adatklasztereit szigorú időrendi sorrendben lévő blokkokba rendezik.

Ahogy a 7. ábrán látható, ezek a blokkok időbélyegzővel rendelkeznek és egy kiválasztott kriptográfiai kivonat azonosítja őket. Minden blokk rendelkezik egy hivatkozással az őt megelőző blokkra, így a blokkok egy visszafelé mutató láncból álló listába rendeződnek, ami a legrosszabb esetben is feldolgozható már az első blokktól kezdve, és egyértelműen meghatározható belőle az elosztott adatbázis aktuális állapota. Természetesen ennek feltétele a blokklánc csomópontjai közt lévő konszenzus. Ha hálózaton belül terjedni kezdenek egy lánc inkonzisztens másolatai, az ellentmondást jellemzően a bányászcsomópontok által alkalmazott egyik követő konszenzus protokollon keresztül oldják fel: *proof-of-work* (POW), *proof-of-stake* (POS) vagy *round-robin* (bányászati diverzitás).

[7] Andrea Pinna – Wiebe Ruttenberg: *Distributed ledger technologies in securities post-trading revolution or evolution?* ECB Occasional Paper 172, April 2016.



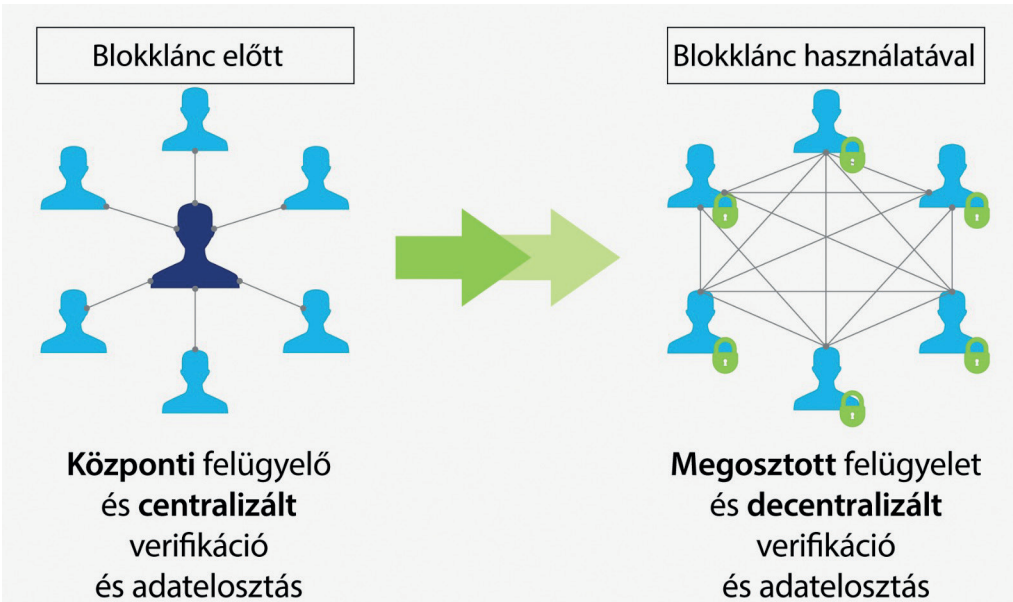
7. ábra: A blokklánc szerkezete
Forrás: Pinna–Ruttenberg (2016) i. m.

A blokklánc-technológia decentralizált természete (8. ábra) semlegesíti egy központi felügyelő vagy ellenőrzőpont szükségességét, amely egy tisztességesebb, biztonságosabb rendszert eredményez. A mód, ahogy az adatot a blokkláncon tárolják, tükrözi a decentralizáltság értékét.[8] Ahelyett, hogy egy központi felügyelőre támaszkodna a többi felhasználóval folytatott tranzakció biztosítására, a blokklánc innovatív konszenzusprotokollokat használ a csomóponthálózaton, hogy kiegyensúlyozottan hitelesítse a tranzakciókat és tárolja az adatokat. Tehát a blokkláncot nem egy központi adatvezérlő tárolja, hanem számos számítógép. A biztonságos és megváltoztathatatlan, kiegyensúlyozott adattárolási és -elosztási mód a blokkláncot olyan eszközzé teszi, amely korlátlan potenciállal rendelkezik a kiberbiztonság és egyéb katonai alkalmazások terén. Hogy megismerhessük azokat a blokklánc-technológiákat, amelyeket a taktikai erők fenntartásának kihívásai során felhasználhatunk, Kovács László azt javasolja, hogy a honvédség tanulmányozza a blokklánc olyan lehetséges megoldásait a kihívásokra, amelyek összefüggenek a szállí-

[8] Gerald P. Dwyer: The economics of bitcoin and other private digital currencies. *Journal of Financial Stability,* 17. (2015), C. 81–91.

tás közbeni láthatósággal, az adatintegritással, beszámolással, a műveleti szerződésekkel és a logisztikai becslésekkel.[9]

McAbee, Tummala és McEachen végzett egy kutatást, amelyben a „katonai hírszerzés-specifikus irányvonalak" keretrendszereinek számos példáját vették alapul, mérlegelve a blokklánc-technológia átvételét. A szerzők meghatározták azt a kulcsfontosságú tulajdonságot, amelyet kötelező érvényűnek tartottak, ez pedig az az együttműködő folyamat, amelyben számos résztvevő közt oszlik meg az irányítás. Peck modellje rugalmasságot mutat a következőben: „potenciális alkalmazhatóság, ami arra enged következtetni, hogy még egyéb el nem fogadható tényezők jelenléte mellett is a blokklánc-technológia megfontolásra érdemes olyan esetekben, ahol valószínűsíthető, hogy az adatbázist támadás éri."[10] A katonai hírszerzés számára olyan esetekben válna ez kimondottan hasznossá, amikor megtörténik a legrosszabb forgatókönyv, tehát „a rendszerműveleteket célzó kiber-, elektromágneses- vagy fizikai támadás kísérlete esetén […] lesz ezekre a legnagyobb szükség".[11]



8. ábra: Centralizált vagy decentralizált adatelosztás
Forrás: Wimal Perera[12]

[9] Kovács László: National cybersecurity strategy framework. *AARMS,* 18. (2019), 2. 65–76.
[10] Ashley McAbee – Murali Tummala – John McEachen: *Military intelligence applications for blockchain technology.* Hawaii International Conference on System Science, 2019.
[11] McAbee–Tummala–McEachen (2019) i. m.
[12] Wimal Perera*:* Understanding blockchain – How it works. *The Capital,* May 13 2019.

A katonai hírszerzési rendszerek biztonsági réseinek azonosítása

Sam Mire, a Disruptor Daily piackutatási elemzője azt állítja, hogy vannak, akik úgy hiszik, az amerikai hadsereg ellátási lánca, kiberbiztonsági rendszere és belső kommunikációja terén hasznot hozna a blokklánc-technológia szemléletének alkalmazása. „Most, hogy a világ láthatóan pengeélen táncol, és az Amerikai Egyesült Államok katonai ereje hanyatlani látszik, hasznos célnak tűnik annak vizsgálata, hogyan hasznosítható a blokklánc védelmi célokra."[13]

Tekintve, hogy az Egyesült Államok katonasága eddig képtelen volt létrehozni a „tökéletes" kommunikációs rendszert, és az olyan kommunikációs programok, mint a Közös Harcászati Rádiórendszer (*Joint Tactical Radio System* – JTRS) több szempontból is elmaradtak az elvárttól,[14] a blokklánc-technológia további vizsgálata a lehetséges katonai célú felhasználásra a következőket foglalja magában:

- *A kiadások, szállítmányok és szerződések jobb láthatósága és nyomon követhetősége* – a blokklánc átlátható elosztott főkönyvi technológiájának használatával a hírszerzés és a védelmi igazgatás kiküszöbölheti a csalásokat, a pazarlást, és csökkentheti a veszteségeket. A Pentagon, becslések szerint, 2,7 milliárd dollár könyv szerinti értékű eszközállománnyal rendelkezik, de 2018-ban az első hivatalos könyvvizsgálói auditja sikertelen volt. Az Ernst & Young egyike volt azoknak a magáncégeknek, amelyeket felkértek az audit lebonyolítására, és nem tudta a feladatot elvégezni, mert „a Védelmi Minisztérium pénzügyi feljegyzései olyan szinten hemzsegtek a hiányosságoktól, pontatlanságoktól és hibáktól, hogy egy megbízható audit lefolytatása egész egyszerűen lehetetlen".[15]
- *A harctéri üzenetek titkosítása* – 2017-ben Ron Wyden, az Egyesült Államok szenátora abbéli aggodalmát fejezte ki, hogy a Védelmi Információs Rendszerek Ügynöksége (*Defense Information Systems Agency* – DISA) nem alkalmaz titkosítási technológiákat a mindennapi kommunikáció során, továbbá rámutat arra is, hogy még az olyan techóriások is, mint a Google és a Facebook standard STARTTLS titkosítási technológiát használ.[16] A társközi üzenetkezelési modell példájaként a Bitcoint lehet említeni, amely minden egyes üzenetet elküld a világ minden aktív csomópontjának másodpercek alatt, és a bitcoinhálózat minden csomópontja hozzájárul ehhez a szolgáltatáshoz, még az okostelefonok is. Ha egy csomópont vezetékes, vezeték nélküli vagy műholdas internetkapcsolata megszakad, a bitcoin-üzenet alternatív csatornákon is elküldhető, például magas frekvenciájú rádión, faxon vagy akár vonalkódalapú üzenet formájában is manuálisan. A fogadáskor a kiszolgáló csomópont ellenőrzi az üzenetet, és továbbítja minden kapcsolódó résztvevőnek.

[13] Sam Mire: Blockchain for military defense: 7 possible use cases. *Disruptor Daily,* 9 November 2018.
[14] David Axe: Failure to communicate: Inside the army's doomed quest for the 'perfect' radio. *The Center for Public Integrity,* January 10, 2012.
[15] Dave Lindorff: Exclusive: The Pentagon's massive accounting fraud exposed. *The Nation,* November 27, 2019.
[16] Ron Wyden (DISA STARTLSS, a DISA igazgatójának továbbított közlemény, 2017. március 22. Online: www.documentcloud.org/documents/3527403-Ron-Wyden-DISA-STARTTLS-Letter-March-22.html

A csomópontok egymástól függetlenül is képesek az üzeneteket blokká alakítani.[17] Végezetül a konszenzusprotokoll biztosítja, hogy az engedély nélküli operátorok érvénytelen üzenetei és blokkjai figyelmen kívül maradjanak. Összességében ezek a protokollok biztosítják azt, hogy a hitelesített forgalom megbízhatóan továbbítható a világ bármely részére, még akkor is, ha a kommunikációs útvonalakat, az egyes csomópontokat vagy magát a blokkláncot támadás éri. A kiberfölényt nem az individuális csomópontok tartják fenn, az egész hálózati rendszer vezérlés alatt tartható aktuális és várt adatokkal.[18]

- *A védelem és a felkészültség növelése a kiberhadviseléssel szemben* – a Defense Advanced Research Projects Agency (DARPA) jelenleg a blokklánc elosztott konszenzusprotokollját vizsgálja, hogy „a kiberbiztonságot agilis és ellenálló védelmi állássá fejlesszék".[19] Donald Trump, az Amerikai Egyesült Államok elnöke 2017 decemberében aláírt egy törvénytervezetet, amely tartalmazott egy rendeletet a blokkláncalapú kiberbiztonság felmérésére „az idegen hatalmak, szélsőséges szervezetek és bűnszervezetek erőfeszítéseiről a hasonló technológiák alkalmazására vonatkozóan; […] és hogy felmérjék az ilyen technológiák jelenlegi vagy tervezett felhasználását a Szövetségi Kormány vagy a kritikus fontosságú infrastrukturális hálózatok berkein belül".[20]
- *A hadászati gyártási folyamatok fejlesztése* – a Naval Additive Manufacturing (Tengerészeti Additív Gyártás) részlege tökéletes használati esete volt a blokklánc-technológiának, amely megmutatta a technológia „képességét hogy titkosítsa és biztonságosan elossza az adatokat az egész gyártási folyamat során (a tervezéstől a prototípuson, a tesztelésen és a gyártáson át egész az átadásig)".[21] Az additív gyártás minden fázisa az adathasználat körül forog, vagy más szóval egy „digitális szál körül: ami egyetlen folyamatos adatszál, ami a kezdeti tervezési elképzeléstől egész a késztermékig nyúlik, felépítve azt az információt, amely lehetővé teszi a tervezést, a modellezést, a gyártást, a felhasználást és az egyes legyártott alkatrészek megfigyelését".[22]
- *A nemzetközi ellátási láncok adatintegritásának védelme és elősegítése* – a blokklánc-technológia képes kiemelni és észlelni a feltörési és behatolási kísérleteket a rendszerbe. Ez nemzetközi fegyverkezési versenyhez vezetett Kína, az Amerikai Egyesült

[17] Melanie Swan: *Blockchain: Blueprint for a new economy.* Newton, O'Reilly Media. 2015.
[18] Haig Zsolt: Connections between cyber warfare and information operations. *AARMS,* 8. (2009), 2. 329–337.
[19] *DoD Digital Modernization Strategy.* DoD Information Resource Management Strategic Plan FY19–23, 2019.
[20] Nemzetbiztonsági Törvény a 2018-as pénzügyi évre, H. R. 2810, 115. kongresszus (2017–2018). Online: www.congress.gov/bill/115th-congress/house-bill/2810
[21] Jon McCarter: *DON innovator embraces a new disruptive technology: blockchain*. SECNAV, United States Navy, 2017.
[22] Abdalla R. Nassar – E. W. Reutzel: *A proposed digital thread for additive manufacturing.* Conference: Solid Freeform Fabrication Symposium Proceedings, Austin, University of Texas, 2013.

Államok és Oroszország között, amelyek próbálják az ellátási láncokon és az adatintegritáson belüli sebezhetőségi problémákat megoldani. A DISA volt igazgatója, Alan R. Lynn altábornagy szerint „néhány éve még, ha egy internetes hozzáférési pontot egy 1-2 gigabájtos támadás ért, az nagy dolognak számított. Most 600 gigás támadások érik az internetes hozzáférési pontokat, és olyan egyedi, különféle támadási módokon, amelyekre korábban még csak nem is gondoltunk. Itt van hát, amit úgy hívunk, hogy »a halál terabájtja« – egy terabájtnyi halál, ami a kapuk előtt ólálkodik."[23] Sok fegyverrendszert 30 éves, vagy még annál is hosszabb életciklusra terveztek. Azonban a számítógépes technológiák, amelyeket a rendszerekhez használtak, sokkal rövidebb felhasználhatósági ciklussal rendelkeznek, ami ritkán nyúlik messzebbre egy évtizednél. Ennek eredményeképpen az elavult alkatrészek cseréje idővel egyre nehezebbé válik. Sőt, számos országban törvény tiltja, hogy olyan komponenseket használjanak, amelyek származását nem lehet igazolni. A tulajdonlás elvesztésével az alkatrészek használhatatlanná válnak, még akkor is, ha azok működőképesek és nagy rájuk a kereslet. Ezzel a viszonteladóknak gazdasági érdekük lett, hogy nyomon kövessék a beazonosított, rendelkezésre álló kereskedelmi komponenseiket egy blokkban, hogy megőrizhessék a származást igazoló adatokat, ami növeli az értéket. A Magyar Honvédség berkein belül nem foglalkoznak külön a decentralizált technológiákkal, de már folyik nemzetközi kutatás és fejlesztés. A NATO-n belül a Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) rendszer, az Egyesült Államok Védelmi Minisztériumán belül pedig a DARPA már hozzáfogott a saját blokkláncprogramjához, biztonságos, decentralizált üzenetkezelési alkalmazást fejlesztve a katonaság számára SBIR 2016.2 név alatt.[24]

– *A fegyverrendszerek védelme* – a haditengerészet Aegis fegyverrendszere (*Aegis Weapon System* – AWS) egy „centralizált, automatikus vezetési és irányítási (C2) és fegyvervezérlő rendszer", amely sebezhető a kibertéri hackertámadásokkal és egyéb veszélyekkel szemben. A kihívások egy ilyen hatalmas fegyver irányítása során akkor kezdődnek, amikor mérlegelésre kerül, hogy pontosan miket kellene a rendszernek egyidőben kezelnie: egy tipikus romboló, mint például az „Arleigh Burke-osztály, az SPY-1 fejlesztett, multifunkciós, fázisrácsvezérelt antennájú lokátorral rendelkezik, MK 41 függőleges rakétaindító rendszerrel és fejlett tengeralattjáró-elhárító fegyverzettel, fejlett légvédelmi rakétákkal és Tomahawk cirkálórakétákkal is rendelkezik szárazföldi célpontok ellen".[25] Ahogy a britek bizonyítottan bevált, felsőbbrendű fegyverintegrációja is győzedelmeskedett a nagyobb tűzerő felett a skagerraki csatában 1916-ban az I. világháború alatt, úgy tud a blokklánc-technológia

[23] Lisa Ferdinando: Terabyte of death' cyberattack against DoD looms, DISA director warns. *U.S. Dept of Defense,* January 11, 2018.

[24] Ashfaq Ahmad Malik et alii: *Application of Cyber Security in Emerging C4ISR Systems and Related Technologies*. Evaluation of OLSR Protocol Implementations Using Analytical Hierarchy Process (AHP). 2014. 224–259.

[25] Arleigh Burke-Class (Aegis) Destroyer. *Naval Technology,* 2020.

> is zökkenőmentesen integrálni és vezérelni számos fegyverrendszert a decentralizált és elosztott architektúrája által.[26] A DARPA 2016-ban egy 1,8 millió dolláros szerződés keretében felkérte a Galois and Guardtime Federalt, hogy „hitelesítsék a Guardtime Federal Kulcsnélküli Aláírás Infrastruktúráját (Keyless Signature Infrastructure), ami teljes egészében egy blokkláncalapú, rendszerintegritást monitorozó megfigyelő rendszer".[27]

McAbee, Tummala és McEachen tanulmányában megemlített elvek ellenőrzőlistaként is szolgálhatnak, ha egy honvédség át szeretne térni a blokklánc használatára. A szerzők a következőket javasolják: amennyiben egy rendszer megfelel az első kiemelt dogmának, kötelező elvnek és még legalább egynek a többi közül, akkor valószínűsíthető, hogy minősített blokklánctechnológia-megoldásként használható modell lesz. A szerzők azt is állítják, hogy egy ilyen modell fejlődni fog a tanulmány alatt.[28] Kovács rávilágít számos kihívásra a *National Cyber Security as the Cornerstone of National Security* című írásában, kitérve az „infrastruktúra gyors modernizációjára" és arra, hogy ez súlyosbítja-e a „létfontosságú infrastruktúra sebezhetőségét", ahogy kitér a közszféra és a magánszektor közös szerepére is.[29] Ezeknek a kihívásoknak a leküzdésére Kovács az Egyesült Királyság nemzeti kiberbiztonsági stratégiáját idézi, miszerint „a kormánynak egyértelmű vezető szerepe van, de ösztönzünk egy szélesebb körű kereskedelmi ökoszisztémát is, felismerve, hogy az ipar hol képes gyorsabb újításokra, mint mi. Ez együtt jár azzal is, hogy a legélesebb fiatal elméket a kiberbiztonsághoz vonzzuk."[30]

Gépi tanulás és mesterséges intelligencia (MI)

A mesterséges intelligencia kifejezést elsőként John McCarthy, az MI atyja használta egy dartmouthi konferencián 1956-ban.[31] A technológia egyik következménye a Project Maven, amelyet Algorithmic Warfare Cross-Function Team néven is emlegetnek, és 2017 áprilisában indult a légierő altábornagyának, Jack Shanahannak a vezetése alatt. A Project Maven fő célja az volt, hogy „integrálják a mesterséges intelligenciát és a gépi tanulást" a nemzetvédelmi műveletekkel, azon belül pedig, hogy „a nemzetvédelem számára rendelkezésre álló hatalmas adatmennyiséget gyorsan bevethető hírszerzési információvá

---

[26] Salvatore Babones: Smart 'Blockchain Battleships' are right around the corner. *The National Interest,* May 17, 2018.

[27] Galois and guardtime federal awarded $1.8 million DARPA contract to formally verify blockchain-based integrity monitoring system. *Galois.com,* September 13, 2016.

[28] McAbee–Tummala–McEachen (2019) i. m.

[29] Kovács László: National cyber security as the cornerstone of national security. *Land Forces Academy Review,* 23. (2018), 2. 114.

[30] *National Cybersecurity Strategy 2016–2021.* HM Government, 2016.

[31] Veronica Adriana Popescu – Gheorghe Popescu – Cristina Raluca Popescu: The amazing world of the internet-challenges of the internet age. *Manager Journal,* 12. (2010), 1. 13–23.

alakítsák.[32] A Mavent arra tervezték, hogy „értelmezze a videós képalkotást, amit aztán a dróntámadások célzóképességének a javítására lehet használni", és hogy mélytanulást és neurális hálózatokat használjanak a folyamatos fejlődéshez. Habár a projekt elismerő kritikát kapott, „a hatalmas szervezeti, etikai és stratégiai kihívások" megmaradtak, és a Maven hamarosan erősen vitatottá vált, amikor több mint 3000 Google-alkalmazott petíciót írt alá, hogy tiltakozzanak az ellen, hogy a vállalat részt vállalt az Egyesült Államok Védelmi Minisztériumának mesterségesintelligencia-kutatásában.[33] Azóta a projekt átkerült a Palantir hatáskörébe.

Az egyik fő probléma, amivel a világ kormányainak szembe kell nézniük, a hagyományos örökölt vezérlésű és működtetésű keretrendszerek integrálása az újabb technológiákkal. Jó példa erre a 20. század első negyedében fejlesztett harckocsik esete, ami végeredményül a „lopakodó és precíziós célzású fegyverek technológiájának" fejlesztéséhez vezetett az 1970-es években. Az ilyen technológiák teremtették meg „a monopólium alapját, majdnem négy évtizeden keresztül, olyan technológiák terén, amelyek gyakorlatilag garantálták a győzelmet bármilyen nem nukleáris háborúban".[34] A drónok által szállított felvételek mennyisége olyan hatalmas, hogy emberi elemző már a puszta mennyiséggel sem tud lépést tartani. Ezért mesterséges intelligenciát használnak, és a gépi tanulásnak köszönhetően az MI folyamatosan fejlődik a célpontok felismerésében és osztályozásában.

Napjainkban legalább 90 ország rendelkezik drónokkal, ideértve a nem állami szerveződésű csoportokat is. Habár ezek legtöbbjét robotikai értelemben nem nevezhetnénk kifinomultnak, ezek közül sokat több száz, sőt több 1000 kilométerre lévő operátorok irányítanak. Az önirányítás egyre inkább észrevehető szerepet kap különféle járművek vezérlésében, főleg a katonaság berkein belül. Például a G-NIUS által kifejlesztett Guardium egy olyan izraeli, személyzet nélküli terepjármű (*Unmanned Ground Vehicle* – UGV), amely „több mint 300 kilogramm kamerát, elektronikai érzékelőt és fegyvert" szállít és használ ütközetben és védelmi célokra a Gázai övezet határvidéke mentén. Habár a jármű önműködő, továbbra is a katonák felelősek a fedélzetén lévő fegyverekért.[35]

Paul Scharre amerikai biztonsági szakértő úgy véli, hogy a mesterséges intelligencián alapuló alkalmazásoknak nincs szükségük jelentős módosításokra, hogy katonai feladatokat láthassanak el, és pont olyan könnyedén integrálhatók fegyverrendszerekbe is, ahogy a polgári megoldásokhoz.[36] Több ország a saját mesterséges intelligenciáin

[32] Timothy Bretl – Ludovic Righetti – Raj Madhavan: Epstein, Project Maven, and some reasons to think about where we get our funding. *IEEE Robotics & Automation,* 26. (2019), 4. 8–13.

[33] Penny Crofts – Honni van Rijswijk: Negotiating 'Evil': Google, Project Maven and the Corporate Form. *Law, Technology and Humans,* 2. (2020), 1. 75–90.

[34] Gregory C. Allen: Project Maven brings AI to the fight against ISIS. *Bulletin of the Atomic Scientists,* December 21, 2017.

[35] John Reed: Israel's killer robot cars. *Foreign Policy,* November 20, 2012.

[36] Paul Scharre: Killer robots and autonomous weapons with Paul Scharre. *Council on Foreign Relations,* June 1, 2018.

alapuló technológiáját teszteli katonai célokra, de „komoly emberi jogi, etikai és nemzetközi normákat érintő aggályok merültek fel”.[37]

Mesterséges intelligencia és rendvédelem

2018 júliusában Daniel Faggella, az Emerj MI Kutatási Intézet kutatási vezetője és vezérigazgatója felszólalt az Interpol és az ENSZ (UNICRI) globális találkozóján, amelynek témája a rendvédelmi szervek számára fejlesztett mesterséges intelligencia és robotika által nyújtott lehetőségek és az abban rejlő kockázatok volt. Ezzel kezdődött az a párbeszéd, amely a mesterséges intelligencia felhasználásával foglalkozott rendészeti, biztonsági és rendvédelmi vonatkozásban. Fontos megállapításokat tettek a szakemberek az UNICRI jelentésben, amelyet a mesterséges intelligencia integrálásáról írtak a rendvédelmi szektorba.

Kevin McCaney azt írja, hogy a rendvédelmi ügynökségek egyre inkább kezdenek prediktív elemzőszoftverekre támaszkodni a bűnmegelőzés során. Egészen mostanáig ezeket a technológiákat jellemzően a versenyszféra nagyvállalatai használták. Erre példa az IBM Blue Crush *(Criminal Reduction Utilizing Statistical History)* szoftvere, amelyet a Tennessee állambeli Memphis rendőrsége használ arra, hogy „elemezze a bűnözési és letartóztatási adatokat, összevesse azokat az időjárás-jelentésekkel, gazdasági tényezőkkel és az olyan eseményekhez kötődő információkkal, mint fizetésnap vagy koncertek, hogy létrehozzanak egy előrejelző-modellt”.[38] A rendőrség, a bíróságok és a büntetőintézetek közösen dolgoznak azon, hogy formálják a büntetőjogi és igazságszolgáltatási rendszert. Az optimális szintű teljesítmény érdekében ezeknek a szervezeteknek olyan szakértőkkel kell rendelkezniük, akik képesek elemezni a bűnözési adatokat, és képesek forgatókönyveket szimulálni, amelyekkel növelhetik a mesterséges intelligenciát használó programok pontosságát. Erre példa a Nemzeti Hírszerzési Modell (*National Intelligence Model* – NIM) az Egyesült Királyságban, amelyet arra terveztek, hogy fejlessze és segítse a hírszerzésre támaszkodó rendőrséget. A NIM kilenc különálló elemből áll:[39]

1. bűnözési sablonok (számok/kapcsolatok);
2. bűnügyi felmérések;
3. demográfiai/társadalmi trendek elemzései;
4. a bűnözői tevékenységek profilozása;
5. hálózatelemzés (résztvevők, akik ilyen hálózatokat építenek ki);
6. kockázatelemzés;
7. célprofilelemzés;

[37] Oriana Pawlyk: If it’s not ethical, they won’t field it: Pentagon release new A. I. guidelines. *Military.com,* 24 February, 2020.
[38] Kevin McCaney: Law enforcement using analytical tools to predict crime. *Gcn.com,* December 22, 2010.
[39] Haitham Hmoud Alshibly – Mohammad Atwah Al-Ma’aitah – Suhaib Alzou’bi: Artificial intelligence in law enforcement. A Review. *International Journal of Advanced Information Technology (IJAIT)*, 4. (2014), 4. 1–9.

8. műveleti hírszerzési felmérés;
9. olyan elemzéseket ad eredményül, amelyek értékelik a különféle rendvédelmi tevékenységek hatékonyságát.

Az UNICRI jelentése arra a következtetésre jutott, hogy az MI és a robotika pont úgy használható fegyverkezési célra, ahogy a közjó érdekében is a rendészet és a bűnmegelőzés terén, és kijelenti, hogy „egy friss jelentésben 14 intézmény (akadémiák, civil szervezetek, ipari szereplők) 26 szerzője mélységeiben vizsgálta meg a kérdést, és arra jutottak, hogy sok olyan jellemzője, ami vonzóvá tenné a mesterséges intelligenciát és a robotikát a rendvédelem számára (például a terjedelem, a sebesség, a teljesítmény és a távolság) pont ilyen vonzóvá teszi a mesterséges intelligenciát és a robotikát a bűnözők és a terroristacsoportok számára is”.[40]

A jelentés három fő támadási területet azonosított:

1. Digitális támadások, mint például automatizált *spear phishing* (személyre vagy csoportra szabott adathalászati támadás), vagy a kiberrendszerek sérülékenységének automatikus felderítése és kihasználása.
2. Politikai támadások, például álhírek vagy médiaanyagok terjesztése zavarkeltés vagy konfliktusokozás céljából, vagy az arccsere *(deep fake)* és egyéb hamisító eszközök alkalmazása videók manipulálására és a politikai szereplőkbe vetett bizalom megingatására, ami akár azt is eredményezheti, hogy a bíróság előtt bemutatott bizonyítékok hitelessége is megkérdőjeleződik.
3. Fizikai támadások, például a felfegyverzett drónok arcfelismerő képessége vagy a csempészdrónok. A digitális támadások kontextusában a jelentés kitér arra is, hogy az MI alkalmazható arra, hogy közvetlenül vigyen végbe káros cselekedeteket, vagy hogy más mesterséges intelligencián alapuló rendszernek ártson mérgezett adatkészletekkel.[41]

Összegzés

A blokklánc és a mesterséges intelligencia megjelenésével a honvédség, a katonai hírszerzés és a védelmi igazgatás legfőbb szervezetei képesek hatékonyabb döntéshozatali előkészítő teljesítményre, nagyobb mennyiségű adatok és összefüggések elemzésére, biztonságosabb módon. Az új technológiákra alapuló megoldások a minősített adat- és információs kommunikációban, valamint az emberi mértékkel már kezelhetetlen mennyiségű információ összegzésében, elemzésében tudnak képességeket növelni. Ez a képességfejlesztés időben és döntéshozatalban mérhető, ami akár közvetett módon emberéletek megóvását is jelentheti. Az *Accenture* által publikált kutatási beszámoló szerint „hét közül hat (86%) repülési és védelmi vállalat tervezi azt, hogy integrálja

[40] Radhika Madhavan: Artificial intelligence in policing – Use-cases, ethical concerns, and trends. *Emerj.com,* December 16, 2019.
[41] Mark T. Simerly – Daniel J. Keenaghan: Blockchain for military logistics. *Army.mil,* November 4, 2019.

a blokkláncot három éven belül", míg „a repülésügyi és védelmi cégvezetők 93%-a hiszi úgy, hogy a következő generációs intelligens megoldások a fizikai környezetbe lépnek".[42] Amikor egy nemzet úgy dönt, hogy szövetségi szinten fejleszti és/vagy korszerűsíti kiberbiztonsági stratégiáit, számos kihívással és dilemmával kell szembenéznie a különféle megközelítések és irányelvek tükrében felmerülő aggályokkal, illetve ezeknek a kiberbiztonsági kihívásoknak a lehetséges kezelési módjaival kapcsolatban.

Mivel a kibertér ilyen exponenciális sebességgel növekszik, a NATO és az Európai Unió is saját alapelveket hozott a kiberbiztonságra vonatkozóan. A NATO vonatkozásában a kiberbiztonsági alapelvek és szabályozások a következőket foglalják magukban:

- ha a kibertérre háborús színtérként tekintünk, annak számos következménye van a tagállamokra nézve (például szélesebb körű kibervédelmi feladatokat kapnak a hadseregek, kibertámadási képességeket kell kiépíteni, és fel kell állítani a kiberparancsnokságot);
- a NATO Kibervállalásának *(Cyber Pledge)* egyik pontja, hogy közelebb hozza a tagállamok egymástól eltérő kiberbiztonsági szintjét;
- a NATO Kiberműveleti Központja fontos szerepet játszhat nemcsak katonai téren, de a polgári védelmi szektorban is (NATO 2020).[43]

A Szövetség javasolja a nemzetközi közreműködés erősítését a tagállamok és a nem NATO-tagországok közt egyaránt.

A blokklánc-technológia ezenfelül visszájára fordítja az adatbiztonsági paradigmát. Először is megbízható, mivel a belső és a külső felhasználóknak is jóváhagyással kell rendelkezniük a hálózaton. Másodszor átláthatóan biztonságos, és nem függ a hibásan működő csomópontoktól, sokkal inkább kriptográfiai adatszerkezetekre támaszkodik, ami hihetetlenül összetetté és azonnal láthatóvá teszi. Végezetül a blokkláncháló hibatűrő, összehangolja a megbízható csomópontokat, ami azt jelenti, hogy a megbízhatatlan feljegyzéseket elveti. Ennek eredményeképpen a blokklánc nemcsak a hiba valószínűségét csökkenti, de jelentősen megnöveli az idegen felek betörési kísérleteinek költségét is.

Ajánlott, hogy a központi védelmi szervek organikus szakértelemre tegyenek szert a blokklánc-technológia terén, és erős kapcsolatot létesítsenek az iparral, hogy ezekből a kölcsönösségen alapuló kapcsolatokból fejleszthessék a blokkláncalapú technológiákat, mindkét fél kölcsönös előnyére.

A folyamatosan fejlődő kibervilág szigorúbb szabályozást és számonkérhetőséget igényel. Ahogy a fejlett országok próbálnak megbirkózni a kibervilághoz kapcsolódó kihívások özönével, a fejlődő országoknak is fel kell készülniük, mivel minden ország elsődleges kötelessége az emberek védelme. A blokklánc-technológia és a mesterséges intelligencia megadja a kulcsot az okosabb és biztonságosabb kiberbiztonsági rendszerekhez.

---

[42] Aerospace and defense technology vision 2018. *Accenture.com,* 2018.

[43] Cyber defence. *North Atlantic Treaty Organization,* 25 September, 2020.

Felhasznált irodalom

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

Aerospace and defense technology vision 2018. *Accenture.com,* 2018. Online: www.accenture.com/_acnmedia/PDF-79/Aerospace-Defense-Tech-Vision-2018.pdf

Allen, Gregory C.: Project Maven brings AI to the fight against ISIS. *Bulletin of the Atomic Scientists,* December 21, 2017. Online: https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/

Andersen, Jesper Carvalho: The great chain of being sure about things. *The Economist,* October 31, 2015. Online: www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things?fsrc=scn%2Fli%2Fte%2Fpe%2Fed%2Fthegreatchainofbeingsureaboutthings

Arleigh Burke-Class (Aegis) Destroyer. *Naval Technology,* 2020. Online: www.naval-technology.com/projects/burke

Axe, David: Failure to communicate: Inside the army's doomed quest for the 'perfect' radio. *The Center for Public Integrity,* January 10, 2012. Online: https://publicintegrity.org/national-security/failure-to-communicate-inside-the-armys-doomed-quest-for-the-perfect-radio/

Babones, Salvatore: Smart 'Blockchain Battleships' are right around the corner. *The National Interest,* May 17, 2018. Online: https://nationalinterest.org/feature/smart-battleships-are-right-around-the-corner-25872

Bower, Joseph L. – Christensen, Clayton M.: Disruptive technologies: Catching the wave. *Harvard Business Review,* January–February 1995. Online: https://hbr.org/1995/01/disruptive-technologies-catching-the-wave

Bretl, Timothy – Righetti, Ludovic – Madhavan, Raj: Epstein, Project Maven, and some reasons to think about where we get our funding. *IEEE Robotics & Automation,* 26. (2019), 4. 8–13. Online: 10.1109/MRA.2019.2943271

Crofts, Penny – Rijswijk, Honni van: Negotiating 'Evil': Google, Project Maven and the Corporate Form. *Law, Technology and Humans,* 2. (2020), 1. 75–90. Online: https://doi.org/10.5204/lthj.v2i1.1313

Cyber defence. *North Atlantic Treaty Organization,* 25 September, 2020. Online: www.nato.int/cps/en/natohq/topics_78170.htm

DoD Digital Modernization Strategy. DoD Information Resource Management Strategic Plan FY, 19–23, 2019. Online: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

Dwyer, Gerald P.: The economics of bitcoin and other private digital currencies. *Journal of Financial Stability,* 17. (2015), C. 81–91. Online: 10.1016/j.jfs.2014.11.006

Ferdinando, Lisa: Terabyte of death' cyberattack against DoD looms, DISA director warns. *U.S. Dept of Defense,* January 11, 2018. Online: www.defense.gov/Explore/News/Article/Article/1414146/terabyte-of-death -cyberattack-against-dod-looms-disa-director-warns/

Galois and guardtime federal awarded $1.8 million DARPA contract to formally verify blockchain-based integrity monitoring system. *Galois.com,* September 13, 2016. Online: https://galois.com/news/galois-guardtime-formal-verification/

Garstka, John J.: Network-centric warfare offers warfighting advantage. *Afcea.org,* May 2003. Online: www.afcea.org/content/network-centric-warfare-offers-warfighting-advantage

Haber, Stuart – Stornetta, W. Scott: How to time-stamp a digital document. *Journal of Cryptology,* 3. (1991). 2. 99–111. Online: https://doi.org/10.1007/BF00196791

Haig Zsolt: Connections between cyber warfare and information operations. *AARMS,* 8. (2009), 2. 329–337.

Hmoud Alshibly, Haitham – Al-Ma'aitah, Mohammad Atwah – Alzou'bi, Suhaib: Artificial intelligence in law enforcement. A Review. *International Journal of Advanced Information Technology (IJAIT)*, 4. (2014), 4. 1–9. Online: 10.5121/ijait.2014.4401

Kovács László: National cyber security as the cornerstone of national security. *Land Forces Academy Review,* 23. (2018), 2. 113–120. Online: 10.2478/raft-2018-0013

Kovács László: National cybersecurity strategy framework. *AARMS,* 18. (2019), 2. 65–76. Online: 10.32565/aarms.2019.2.9

Lindorff, Dave: Exclusive: The Pentagon's massive accounting fraud exposed. *The Nation,* November 27, 2019. Online: www.thenation.com/article/archive/pentagon-audit-budget-fraud/

Madhavan, Radhika: Artificial intelligence in policing – Use-cases, ethical concerns, and trends. *Emerj.com,* December 16, 2019. Online: https://emerj.com/ai-sector-overviews/artificial-intelligence-in-policing/

Malik, Ashfaq Ahmad – Mahboob, Athar – Khan, Adil – Zubairi, Junaid: *Application of Cyber Security in Emerging C4ISR Systems and Related Technologies*. Evaluation of OLSR Protocol Implementations Using Analytical Hierarchy Process (AHP). 2014. 224–259. Online: 10.4018/978-1-4666-4707-7.ch086

McAbee, Ashley – Tummala, Murali – McEachen, John: *Military intelligence applications for blockchain technology.* Hawaii International Conference on System Science, 2019.

McCaney, Kevin: Law enforcement using analytical tools to predict crime. *Gcn.com,* December 22, 2010. Online: https://gcn.com/articles/2010/12/22/police-predictive-analysis-software.aspx

McCarter, Jon: *DON innovator embraces a new disruptive technology: blockchain*. SECNAV, United States Navy, 2017.

Mire, Sam: Blockchain for military defense: 7 possible use cases. *Disruptor Daily,* 9 November 2018. Online: www.disruptordaily.com/blockchain-use-cases-military-defense/

Nassar, Abdalla R. – Reutzel, E. W.: *A proposed digital thread for additive manufacturing.* Conference: Solid Freeform Fabrication Symposium Proceedings, Austin, University of Texas, 2013.

National Cybersecurity Strategy 2016–2021. HM Government, 2016. Online: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf

Pawlyk, Oriana: If it's not ethical, they won't field it: Pentagon release new A. I. guidelines. *Military.com,* 24 February, 2020. Online: www.military.com/daily-news/2020/02/24/if-its-not-ethical-they-wont-field-it-pentagon-release-new-ai-guidelines.html

Perera, Wimal*:* Understanding blockchain – How it works. *The Capital,* May 13 2019. Online: https://medium.com/the-capital/understanding-blockchain-how-it-works-5772e29421b8

Pinna, Andrea – Ruttenberg, Wiebe: *Distributed ledger technologies in securities post-trading revolution or evolution?* ECB Occasional Paper 172, April 2016. Online: www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf

Popescu, Veronica Adriana – Popescu, Gheorghe – Popescu, Cristina Raluca: The amazing world of the internet-challenges of the internet age. *Manager Journal,* 12. (2010), 1. 13–23.

Reed, John: Israel's killer robot cars. *Foreign Policy,* November 20, 2012. Online: https://foreignpolicy.com/2012/11/20/israels-killer-robot-cars/

Scharre, Paul: Killer robots and autonomous weapons with Paul Scharre. *Council on Foreign Relations,* June 1, 2018. Online: www.cfr.org/podcasts/killer-robots-and-autonomous-weapons-paul-scharre

Simerly, Mark T. – Keenaghan, Daniel J.: Blockchain for military logistics. *Army.mil,* November 4, 2019. Online: www.army.mil/article/227943/blockchain_for_military_logistics

Swan, Melanie: *Blockchain: Blueprint for a new economy.* Newton, O'Reilly Media. 2015.

Tapscott, Don – Tapscott, Alex: *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. New York, Portfolio/Penguin, 2016.

A Katonai Műszaki Doktori Iskolában folyó képzés és kutatás a műszaki tudományterülethez tartozó tudományágaknak a teljes védelmi szektorban történő alkalmazására irányul. A hallgatók tudományos tevékenységüket gyakran több tudományterület és tudományág határterületén művelik, és a kutatásaik során azok interdiszciplináris kérdéseire, szinergiáira fókuszálnak.

Mindezt az ebben a kötetben található írások is igazolják. A szerzők olyan tudományos problémákat feszegetnek, mint például a blokkláncok és a mesterséges intelligencia alkalmazhatósága a kiberhadviselésben, a Mi–24 helikopterek elektronikai hadviselési képességeinek fejlesztése vagy az állami célú adatátviteli rendszerek integrálhatóságának kérdései. A környezetbiztonság és a vízgazdálkodás, valamint a vízbiztonság területéhez köthetően is több írással találkozhatunk a kötetben.