HDR 2021, Nr. 1–2, 4–19.

Viktor Huszár

DISTRIBUTED INTELLIGENCE: CYBER WARFARE APPLICATION POSSIBILITIES OF COMPUTER VISION AND ARTIFICIAL INTELLIGENCE[1]

DOI: 10.35926/HDR.2021.1-2.1

ABSTRACT: *Artificial Intelligence (AI) and blockchain technology have significant transformative potential to create next level solutions in improving traditional systems within military and law enforcement. Despite initial scepticism in scaling blockchain technology beyond the boundaries of digital currencies and overcoming dependence on traditional legacy systems, it is evident that the technology, together with AI has the potential to become greater than the internet itself.*[2] *Countries like China and the United States have expressed interest in applying and combining the technologies for improvements and advancements in military and law enforcement areas, such as "cyber defence, secure messaging, resilient communications, logistics support and the networking of the defence Internet of Things (IoT)".*[3] *As investors and innovators seek to cash in on the merging of two powerful technologies, we have reached the crossroads necessitating a comprehensive research effort to determine best-use cases and utilization practices for military and law enforcement purposes.*

KEYWORDS: *Artificial Intelligence, decentralized, blockchain, security, military, law enforcement, cyber security, machine learning*

INTRODUCTION

The past few decades have illustrated what is already known – information technology is not only evolving but disrupting numerous industries with the potential to offer scalability and advancements at an unprecedented rate. Next generational technologies, such as blockchain and Distributed Ledger Technology (DLT), augmented with machine learning and Artificial Intelligence, offer military and law enforcement the opportunity to transform and further safeguard their respective industries.

As early as the 1990s, the United States employed digital technologies, like *network-centric operations* that merged "tactics, techniques and procedures that a networked force

[1] A tanulmány a TKP2020-NKA-09 számú projekt részeként a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Tématerületi Kiválósági Program 2020 pályázati program finanszírozásában valósult meg. / The study was implemented as part of the project TKP2020-NKA-09 with the support of the National Research Development and Innovation Fund, in the financing of the Thematic Excellence Program 2020 application program.

[2] Hashim, H. "Military Applications of Blockchain Technology." *Fintech News,* 1 July 2020. https://www.fintechnews.org/military-applications-of-blockchain-technology/

[3] Sanchez, S. L. "Blockchain Technology In Defence". *European Defence Matters,* 14. 2017. 17. https://www.eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence

can employ to create a decisive warfighting advantage".[4] In 1995, Bower and Christensen shone a spotlight on "disruptive" technologies that could keep competitors ahead of the competition. Their research illustrated that the majority of well-established companies strive to remain ahead of their respective industries when it comes to "developing and commercializing new technologies" that ranged from step-by-step improvements to unique progressive approaches that turned industries on its head – with the main aim being that such advancements "address the next-generation performance needs of their customers".[5]

Around the same time, a ubiquitous information network appeared based on blockchain technology – a technology that had the potential to secure immutable records without a central authority at the helm.[6] Fast forward decades later and blockchain's DLT is set to impact multiple industries, influence economic systems, legal frameworks and information technologies at large.[7] It must be noted that while commercial industries have rushed to get ahead with respect to blockchain technology, and faced a certain amount of scrutiny regarding the lack of regulations, far less attention has been fixed on the opportunities and vulnerabilities blockchain technology would bring to military intelligence and law enforcement.

The following subsections broadly define blockchain technology to project possible relationships between the technology with respect to implementation and utilization within the military intelligence and law enforcement sectors.

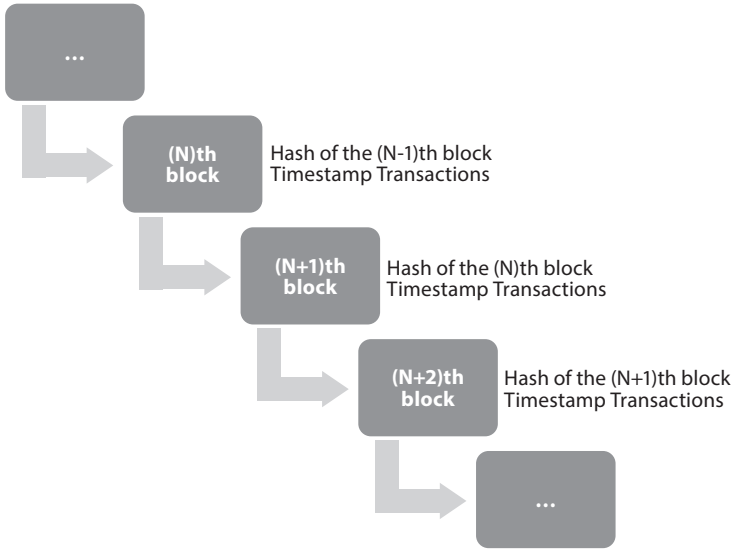

Figure 1 *Structure of Blockchain (Based on Pinna and Ruttenberg, 2016)*

4 Garstka, J. J. "Network-Centric Warfare Offers Warfighting Advantage." *SIGNAL Magazine,* May 2003. https://www.afcea.org/content/network-centric-warfare-offers-warfighting-advantage, Accessed on 20 April 2020.

5 Bower, J. L. and Christensen, C. M. "Disruptive Technologies: Catching the Wave." *Harvard Business Review* 73/1. 1995. 43–53. https://hbr.org/1995/01/disruptive-technologies-catching-the-wave

6 Haber, S. and Stornetta, W. S. "How to time-stamp a digital document." *Journal of Cryptology* 3/2. 1991. 99–111. DOI: 10.1007/bf00196791

7 Andersen, C. "The Great Chain of Being Sure About Things." *The Economist,* 31 Oct 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things, Accessed on 22 May 2020.

BLOCKCHAIN TECHNOLOGY DEFINED

Blockchain is a distributed data storage approach, where "blockchain" describes the list of data clusters (blocks) that are organized into a limitless chain creating a distributed database. Each block contains a link to the preceding block on each node (participant) that the blockchain stores. A basic feature of blockchain systems is the storage of blockchain nodes in sorted entries with unified agreement on the current state using a *consensus* approach. Though this approach to distributed storage has been popularized through Bitcoin's distributed "cryptocurrency" framework, many alternative systems currently exist or are under development which follow the same principle but differ fundamentally in their purpose and key technology. As it stands, these systems are collectively and improperly referred to as "blockchain technology".

It is blockchain's capacity to decentralize transactions while increasing security that has tech entrepreneurs investing in what is most likely the next technological revolution that will greatly impact and transform society, economies, and the internet.[8] The importance of blockchain's distributed fault tolerance and seamless transaction has already been recognized by the military sector and research is under way to determine whether existing systems can be successfully migrated to blockchain, in whole or in part.

In the context of blockchain technologies, the ledger is an entry repository where entries can be stored without possibility of modification once they become part of the database – the ledger may also demonstrate narrow "ledger" semantics depending on the blockchain technologies applied but this is an irregularity. Blockchain technologies implement and expand a distributed ledger through continuous synchronization with nodes in the distributed network. The network can be geographically distant or owned by various companies, so each node has a copy of the ledger. Any additions to the ledger require an agreement by other nodes, followed by the verified block's appearance within minutes or seconds on other nodes, depending on the solutions used. Any trusted central monitoring body can access the information stored in the entries, without involving said body's internal processes and rules.[9]

The ledger is maintained by distributed network nodes based on a number of consensus algorithms employing cryptography to store and verify transactions. This allows the network to remain functional even with a large number of defective nodes, provided that the number of defective nodes is below the maximum allowed. IT applies the distributed consensus algorithm or, more generally, the distributed consensus protocol a great deal. In each application context, the selection of the consensus protocol is influenced by factors such as hypothesized failure modes, maximum system size, consensus response time, and synchronization requirements. Accordingly, it is not surprising that different blockchain technologies utilize several different consensus protocols. What is uniform in blockchain technologies is that the problem of distributed consensus is addressed by some protocol.

Blockchain has a common structure and can be viewed as a transaction log (journal) whose data clusters are stored in blocks in a strictly chronological order. As shown in *Figure 1,* these blocks are time-stamped and identified by selected cryptographic hash. Each block contains a reference to the block preceding it, and in this way, the blocks are

[8] Tapscott, D. and Tapscott A. *Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business, and the World*. London: Penguin, 2016.

[9] Pinna, A. and Ruttenberg, W. *Distributed ledger technologies in securities post-trading: revolution or evolution?* Frankfurt: European Central Bank, 2016. DOI: 10.2866/270533

organized into a backward-chained list which, at its worst, can be processed from the first block to clearly determine the current state of the distributed database. Of course, this implies consensus between nodes on the blockchain. If inconsistent copies of a chain begin to spread within the network, the discrepancy is typically resolved through one of the following consensus protocols applied via mining nodes: proof-of-work (POW), proof-of-stake (POS), or round-robin (mining diversity).

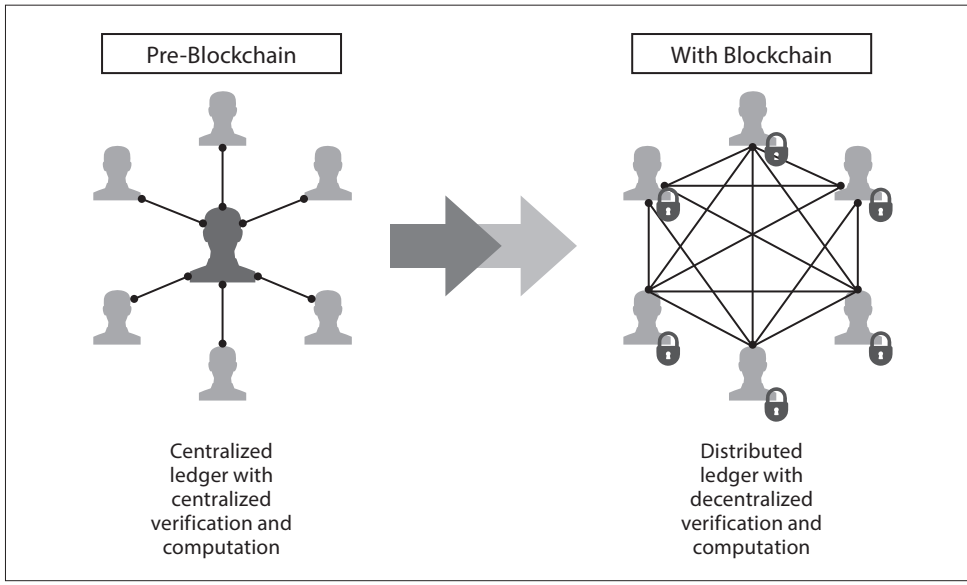

Figure 2 *Centralized v Decentralized Data Distribution*[10]

The decentralized nature of blockchain technology *(Figure 2)* removes the need for a central authority or checkpoint, which ultimately creates a fairer, more secure system. The way data is recorded on the blockchain reflects the value of decentralization.[11] Instead of relying on a central authority to secure transactions with other users, blockchain uses innovative consensus protocols on the node network to authenticate transactions and record data in an unbiased manner. Thus, the blockchain is not stored by a central data controller but numerous computers.

The unbiased manner of recording and distributing secure, immutable data makes blockchain an asset capable of limitless potential with regards to cyber security and other military applications. To understand the range of blockchain technologies for tactical sustainment challenges, László Kovács suggests the military examine the potential of blockchain solutions to challenges associated with in-transit visibility, data integrity, reporting, operational contracting, and logistic estimation.[12]

[10] Perera, W. "Understanding Blockchain: How it works". *The Capital,* 13 May 2020. https://medium.com/the-capital/understanding-blockchain-how-it-works-5772e29421b8, Accessed on 28 May 2020.

[11] Dwyer, G. P. "The Economics of Bitcoin and Other Private Digital Currencies." *Journal of Financial Stability* 17. 2015. 81–91. DOI: 10.1016/j.jfs.2014.11.006

[12] Kovács, L. "National Cybersecurity Strategy Framework." *AARMS* 18/2. 2019. 65–76. DOI: 10.32565/aarms.2019.2.9

Qualities of the:				Problem			Transaction					Participant					Solution				External Factors	
Author	Sector	Type (C: Criteria, F: Flow Chart)	Year	Solvable without Blockchain	Intermediaries	Centralization	Rate	Size/Data Volume	Digital Nature	Privacy Expectations	Strict Immutability Required/Possible	Interdependency	Quantity	Shared Control	Integrity Motivations	Trust Level	System/Software Control	Stand-Alone System	Current Capability	Permission Type	Likelihood of Attack	Regulation Compliance
Greenspan (19)	Blockchain Development	C	15	×	×	×						×	×	×		×				×		
Birch, Brown, Parulava (20)	Finance	F	16										×	×	×					×		
Meunier (21)	Blockchain Development	C	16		×		×	×		×	×		×	×		×	×	×				
Lewis (22)	Blockchain Development	C	17		×	×						×		×								
Peck (23)	Electrical Engineering	F	17	×			×			×			×			×	×			×	×	
Wüst-Gervais (15)	Computer Science	F, C	17		×	×	×						×			×	×			×		
Mulligan (3)	Finance	F	18		×		×	×	×	×	×			×	×	×	×		×	×		×

Figure 3 *Trends in specific consideration points regarding blockchain applicability, highlighted columns indicate those of particular interest in military intelligence applications*[13]

Authors McAbee, Tummala and McEachen undertook the survey of several examples of "military intelligence-specific guidance" frameworks considering adoption of blockchain technology. The authors identified a key quality they deemed mandatory, that being the collaborative process in which several authors shared control. Peck's model illustrated flexibility in "in potential employment, which suggests that even in the presence of other disagreeable factors blockchain technology may be worth considering in cases where the database is likely to be attacked." Military intelligence would benefit keenly during periods of worst-case scenarios "when cyber, electromagnetic and physical attacks attempt to disrupt system operations […] when they will be needed most".

IDENTIFICATION OF VULNERABILITIES WITHIN MILITARY INTELLIGENCE SYSTEMS

Sam Mire, Market Research Analyst at Disruptor Daily, stated that there is belief the US military's supply chains, cyber security and internal communications could benefit from implementing aspects of blockchain technology.

[13] McAbee, A., Tummala, M. and McEachen, J. "Military Intelligence Applications for Blockchain Technology." In *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Honolulu: University of Hawai'i at Mānoa, 2019. DOI: 10.24251/HICSS.2019.726

"With the world seemingly on edge and America's military manpower seemingly on the decline, exploring how blockchain can be used for defence purposes is a worthwhile pursuit".[14]

With the United States military's inability to create a "perfect" communication system thus far, and ambitious communication programs like the Joint Tactical Radio System (JTRS) failing to live up to its potential in more ways than one,[15] further exploration into blockchain technology's potential military applications include the improved visibility and traceability of expenditure, shipments and contracts – through blockchain's usage of transparent Distributed Ledger Technology the military can eliminate fraud, waste and reduction of losses. The United States Pentagon is worth an estimated $2.7 trillion dollars and failed its first official audit in 2018. Ernst & Young, among other private firms hired to perform the audit, could not complete the job due to the fact that the "DoD's financial records were riddled with so many bookkeeping deficiencies, irregularities, and errors that a reliable audit was simply impossible".[16]

Another application possibility of the technology is securing battlefield messaging – as late as 2017, United States Senator Ron Wyden expressed his concerns over the Defence Information Systems Agency's (DISA) lack of implementing encryption technology in daily communications, further noting that tech giants such as Google and Facebook employ standard STARTTLS encryption technology.[17] Using Bitcoin as an example of peer-to-peer messaging model that delivers every message to every active node in the world in seconds, all nodes in the Bitcoin network contribute to this service, including smartphones. If a node's terrestrial, wireless, or satellite internet service is interrupted, a bitcoin message can be sent through alternative channels, such as high-frequency radio, fax, or even barcode-based note, or manually. Upon receipt, the service node checks the message and forwards it to each associated participant. Nodes can independently aggregate messages into new blocks.[18] Finally, the consensus protocol ensures that invalid messages and blocks generated by rogue operators are ignored. Together, these protocols ensure that authenticated traffic can be reliably relayed anywhere in the world, even if communication paths, individual nodes, or the blockchain itself are attacked. Cyber superiority is not individually maintained by the nodes, but the network system can be kept controlled with current and expected data.[19]

The technology can mean an increased protection and preparedness against Cyber Warfare – the Defence Advanced Research Projects Agency (DARPA) is currently looking into blockchain's distributed consensus protocols to "evolve Cybersecurity for an Agile and

---

[14] Mire, S. "Blockchain for Military Defense." *Disruptor Daily,* 9 November 2018. https://www.disruptordaily.com/blockchain-use-cases-military-defence/, Accessed on 22 May 2020.

[15] Axe, D. "Failure to Communicate: Inside the Army's Doomed Quest for the 'Perfect' Radio." The Center for Public Integrity. 10 January 2012. https://publicintegrity.org/national-security/failure-to-communicate-inside-the-armys-doomed-quest-for-the-perfect-radio/, Accessed on 22 May 2020.

[16] Lindorff, D. "Exclusive: The Pentagon's Massive Accounting Fraud Exposed". *The Nation,* 27 November 2018. https://www.thenation.com/article/archive/pentagon-audit-budget-fraud/, Accessed on 22 May 2020.

[17] Wyden, R. *Ron Wyden to Alan R. Lynn, 22 March 2017.* Letter. https://www.documentcloud.org/documents/3527403-Ron-Wyden-DISA-STARTTLS-Letter-March-22.html, Accessed on 17 April 2020.

[18] Swan, M. *Blockchain: Blueprint for a New Economy.* Sebastopol, CA: O'Reilly Media, 2015.

[19] Haig, Zs. "Connections between Cyber Warfare and Information Operations" *AARMS* 8/2. 2009. 329–337. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1900/13haig.pdf, Accessed on 20 April 2020.

Resilient Defence Posture".[20] United States President Donald Trump signed a bill in December 2017 that includes a mandate for a blockchain-based cyber security assessment "of efforts by foreign powers, extremist organizations, and criminal networks to utilize such technologies; … [and] an assessment of the use or planned use of such technologies by the Federal Government and critical infrastructure networks".[21]

It is also expected, that DLTs will result in improvements to the military's manufacturing processes – the Naval Additive Manufacturing Department was a perfect use case for blockchain technology to illustrate its "ability to secure and securely share data throughout the manufacturing process (from design, prototyping, testing, production, and ultimately disposal)".[22] Each key phase in Additive Manufacturing revolves around use of data, or a "Digital Thread: a single, seamless strand of data that stretches from the initial design concept to the finished part, constituting the information that enables the design, modelling, production, use, and monitoring of an individual manufactured part".[23]

Blockchain technology's ability to highlight and detect hacking and network penetration attempts has led to an international arms race between China, the United States and Russia all vying to solve vulnerabilities within supply chains and data integrity. Protecting and promoting data integrity of military supply chains can be therefore another application of DLTs. Ex-DISA Director Army Lt. Gen. Alan R. Lynn stated, "A few years ago, getting a 1-gigabyte or 2-gigabyte attack at the internet access point was a big deal. Now, we get 600-gig attacks on the internet access points and unique, different ways of attacking that we had not thought of before. There's now, we would call it the 'terabyte of death' – there is a terabyte of death that is looming outside the door".[24] Many weapon systems are designed with a life span of 2-3 decades or even more. However, the computing technologies used by these systems have a short shelf life, rarely lasting more than a decade. As a result, replacing obsolete parts becomes more difficult over time. Furthermore, in several countries, it is prohibited by law to use a component whose origin cannot be ascertained. The loss of ownership renders parts unusable, even if they are functional and in high demand. This would give the resellers an economic incentive to track their identified off-the-shelf commercial components in a block to retain their origin, which in turn adds value.

Decentralized technologies are not dealt with separately in the Hungarian Defence Forces, but international research and development is already underway. NATO's C4ISR and the US Department of Defence (DARPA – DoD) have already launched their own block-

[20] "DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23." United States, Department of Defence. 12 July 2019. https://media.defence.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF, Accessed on 17 April 2020.

[21] National Defense Authorization Act for Fiscal Year 2018, H.R. 2810, 115th Cong. (2017–2018).

[22] McCarter, J. "DON Innovator Embraces a New Disruptive Technology: Blockchain". Secretary of the Navy. 22 June 2017. https://www.secnav.navy.mil/innovation/Pages/2017/06/BlockChain.aspx, Accessed on 22 May 2020.

[23] Nassar, A. R. and Reutzel, E. W. "A proposed digital thread for additive manufacturing". In *Proceedings for the 2013 International Solid Freeform Fabrication Symposium*. Austin: University of Texas, 2013. 19–43. http://utw10945.utweb.utexas.edu/Manuscripts/2013/2013-02-Nassar.pdf

[24] Ferdinando, L. "'Terabyte of Death' Cyberattack against DoD Looms, DISA Director Warns". 11 January 2018. https://www.defence.gov/Explore/News/Article/Article/1414146/terabyte-of-death-cyberattack-against-dod-looms-disa-director-warns/, Accessed on 20 April 2020.

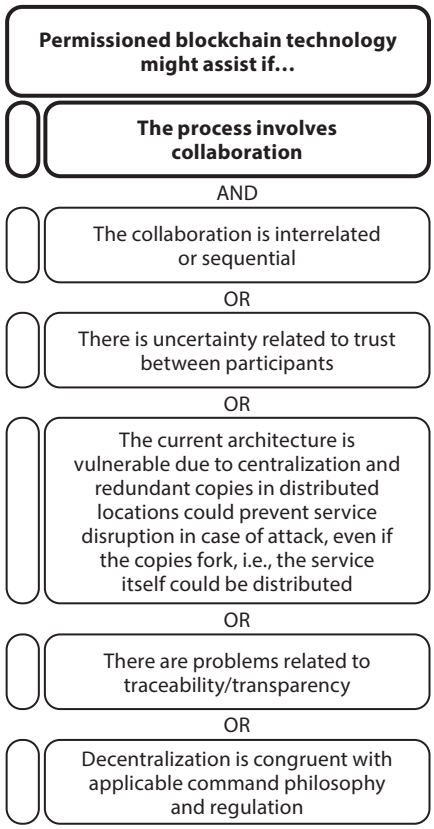

Figure 4 *Critical factors in determining when blockchain technology might apply to military intelligence processes*[29]

chain programs, developing a secure, decentralized messaging application for the military under the name SBIR 2016.2.[25]

All armed forces thrive to protect the weapon systems. The US Navy's' Aegis Weapon System (AWS) is a "centralized automated, command-and-control (C2) and weapons control system" that is vulnerable to cyber hacks and other threats. The challenge in controlling such a powerful weapon arises when you consider exactly what the system is meant to handle simultaneously. A typical destroyer like the "Arleigh Burke Class includes an upgraded SPY-1 multi-function, phased-array radar, Mk 41 Vertical Launching System, an advanced anti-submarine warfare system, advanced anti-air warfare missiles, and Tomahawk land-attack cruise missiles".[26] Much like the British proved superior weapons integration outguns greater firepower in Jutland, 1916 during World War I, blockchain technology can seamlessly integrate and operate multiple weapons' systems through its decentralized and distributed architecture.[27] DARPA awarded Galois and Guardtime Federal a $1.8 million contract in 2016 to "verify the correctness of Guardtime Federal's Keyless Signature Infrastructure (KSI), a formal verification tools and all blockchain-based integrity monitoring systems".[28]

According to McAbee, Tummala and McEachen, *Figure 3* can act like a checklist if the military is interested in adopting blockchain. The authors propose the following: "If a system meets the first, mandatory tenet identified in bold and at least one of the others, it may be a reasonable candidate for a permissioned blockchain technology model". The authors also state that such a model will evolve during the course of the study.

[25] Malik, A. A. et al. "Application of Cyber Security in Emerging C4ISR Systems." In *Crisis Management: Concepts, Methodologies, Tools, and Applications*. Hershey: Information Science Reference, 2014. 1705–1738. DOI: 10.4018/978-1-4666-4707-7.ch086

[26] "Arleigh Burke-Class (Aegis) Destroyer". Naval Technology. https://www.naval-technology.com/projects/burke/, Accessed on 20 April 2020.

[27] Babones, S. "Smart 'Blockchain Battleships' Are Right Around the Corner." *The National Interest,* 17 May 2018. https://nationalinterest.org/feature/smart-battleships-are-right-around-the-corner-25872, Accessed on 22 May 2020.

[28] "Galois and Guardtime Federal Awarded $1.8 Million DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System." Galois. 13 September 2016. https://galois.com/news/galois-guardtime-formal-verification/, Accessed on 20 April 2020.

[29] McAbee, Tummala and McEachen. "Military Intelligence Applications for Blockchain Technology."

Kovács brings to light a number of challenges in his paper, *National Cyber Security as the Cornerstone of National Security,* including that of "the rapid modernization of infrastructure" and whether this exacerbates the "vulnerability of critical infrastructures" as well as the joint roles played by both private and public sectors.[30] To solve these challenges, Kovács quotes from the national cyber security strategy of the United Kingdom, "Government has a clear leadership role, but we will also foster a wider commercial ecosystem, recognising where industry can innovate faster than us. This includes a drive to get the best young minds into cyber security".[31]

MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE (AI)

Project Maven, also known as the Algorithmic Warfare Cross-Function Team, was launched in April 2017 and was overseen by Air Force Lt. Gen. Jack Shanahan. The main goal of Project Maven is to "integrate artificial intelligence and machine learning" into DoD operations and, in particular, to "turn the enormous volume of data available to the DoD into actionable intelligence and insights at speed".[32] Maven was designed to "interpret video imagery, which could in turn be used to improve the targeting capability of drone strikes", and employs deep learning, neural networks to constantly improve. Technologies developed through Maven have already been successfully deployed. Though the Project has received critical acclaim, "enormous organizational, ethical, and strategic challenges" remain where Maven soon became shrouded in controversy when over 3,000 Google employees signed a petition in protest against the company's involvement with a U.S. Department of Defence Artificial Intelligence study.[33] The project has since been taken over by Palantir.

One of the main challenges faced by governments across the world amounts to traditional legacy management and operational frameworks integrating new technologies. An example of this is military tanks developed in the first quarter of the 20th century, and ultimately leading to the development of "stealth and precision-guided weapons technology" in the 1970s. Such technologies created the "foundation for a monopoly, nearly four decades long, on technologies that essentially guaranteed victory in any non-nuclear war".[34] The amount of footage drones provide is so vast that human analysts can no longer cope with the sheer volume. Therefore, artificial intelligence is being harnessed, and thanks to machine learning, AI will constantly improve at recognizing and classifying objects.

Today, at least 90 countries have drones, including many non-state groups. While most of them will not be classified as sophisticated within the field of robotics, many are remotely controlled with operators hundreds, if not thousands of miles away. Autonomy is becoming increasingly apparent in the management of different vehicles, especially those used by the military. For example, the Guardium, developed by G-NIUS, is an Israeli

---

30 Kovács, L. "National Cyber Security as the Cornerstone of National Security." *Land Forces Academy Review* 23/2. 2018. 113–120. DOI: 10.2478/raft-2018-0013

31 Kovács. "National Cyber Security as the Cornerstone of National Security."

32 Bretl, T., Righetti, L. and Madhavan, R. "Epstein, Project Maven, and Some Reasons to Think About Where We Get Our Funding." *IEEE Robotics & Automation* 26/4. 2019. 8–13. DOI: 10.1109/MRA.2019.2943271

33 Crofts, P. and Rijswijk, H. v. "Negotiating 'Evil': Google, Project Maven and the Corporate Form." *Law, Technology and Humans* 2/1. 75–90. DOI: 10.5204/lthj.v2i1.1313

34 Allen, G. C. "Project Maven Brings AI to the Fight Against ISIS." *Bulletin of the Atomic Scientists,* 21 December 2017. https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/, Accessed on 22 May 2020.

unmanned ground vehicle (UGV) that "carries more than 660-pounds of cameras, electronic sensors and weapons" and is used for combat and defence along the Gaza border. Though the vehicle is self-propelled, soldiers continue to be responsible for the weapons on board.[35]

US Security Expert, Paul Sharre believes that Artificial Intelligence applications do not require major modifications to military tasks and can be integrated into weapon systems just as easily as civilian solutions.[36] According to General Shanahan, the United States intends to stand apart from Russia and China. Both countries are currently testing their uses of Artificial Intelligence technology for military purposes, but raise "serious concerns about human rights, ethics, and international norms".[37]

ARTIFICIAL INTELLIGENCE IN LAW ENFORCEMENT

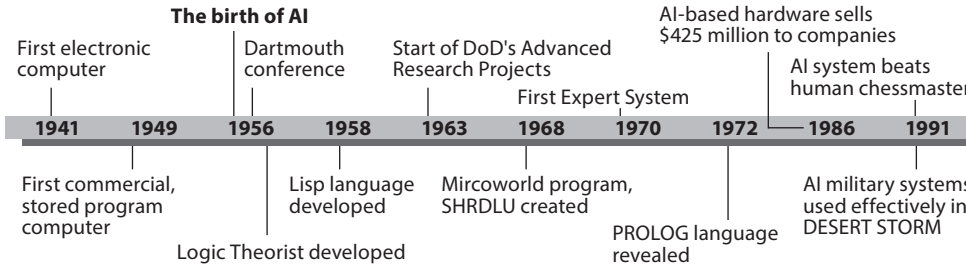

Figure 5 *Timeline of major Artificial Intelligence events (Oracle, 1997)*

Artificial Intelligence was first coined by John McCarthy, also known as the father of AI, at a Dartmouth conference in 1956.[38] Fast forward to July 2018, where Daniel Faggella, the head of Research and CEO of Emerj, addressed the Interpol–United Nations (UNICRI) Global Meeting on the Opportunities and Risks of Artificial Intelligence and Robotics for Law Enforcement. This was the beginning of discussions regarding Artificial Intelligence in policing, security and law enforcement. The following diagram is featured in the UNICRI's report on integrating Artificial Intelligence into the law enforcement sector.

Kevin McCaney notes in *Law Enforcement Using Analytical Tools to Predict Crime,* that law enforcement agencies are starting to rely on predictive analysis software in anticipating and preventing crime. Until recently, such tech was mostly used by competitive enterprises. An example would be the IBM Blue CRUSH (Criminal Reduction Utilizing Statistical History) software in use by the Memphis, Tennessee Police Department to "analyze crime

[35] Reed, J. "Israel's Killer Robot Cars". *Foreign Policy,* 20 November 2012. https://foreignpolicy.com/2012/11/20/israels-killer-robot-cars/, Accessed on 28 May 2020.

[36] Lindsay, J. M. (host). "Killer Robots and Autonomous Weapons With Paul Scharre". Podcast. 1 June 2018. https://www.cfr.org/podcasts/killer-robots-and-autonomous-weapons-paul-scharre, Accessed on 28 May 2020.

[37] Pawlyk, O. "If It's Not Ethical, They Won't Field It: Pentagon Release New A.I. Guidelines". Military.com. 24 February 2020. https://www.military.com/daily-news/2020/02/24/if-its-not-ethical-they-wont-field-it-pentagon-release-new-ai-guidelines.html, Accessed on 23 April 2020.

[38] Popescu, V. A., Popescu, G. and Popescu, C. R. "The amazing world of the Internet-Challenges of the Internet Age". *Manager Journal* 12/1. 2010. 13–23. http://manager.faa.ro/download/536_1202.pdf

and arrest data, and combine it with weather forecasts, economic factors, and information on events such as paydays and concerts to create predictive models".[39]

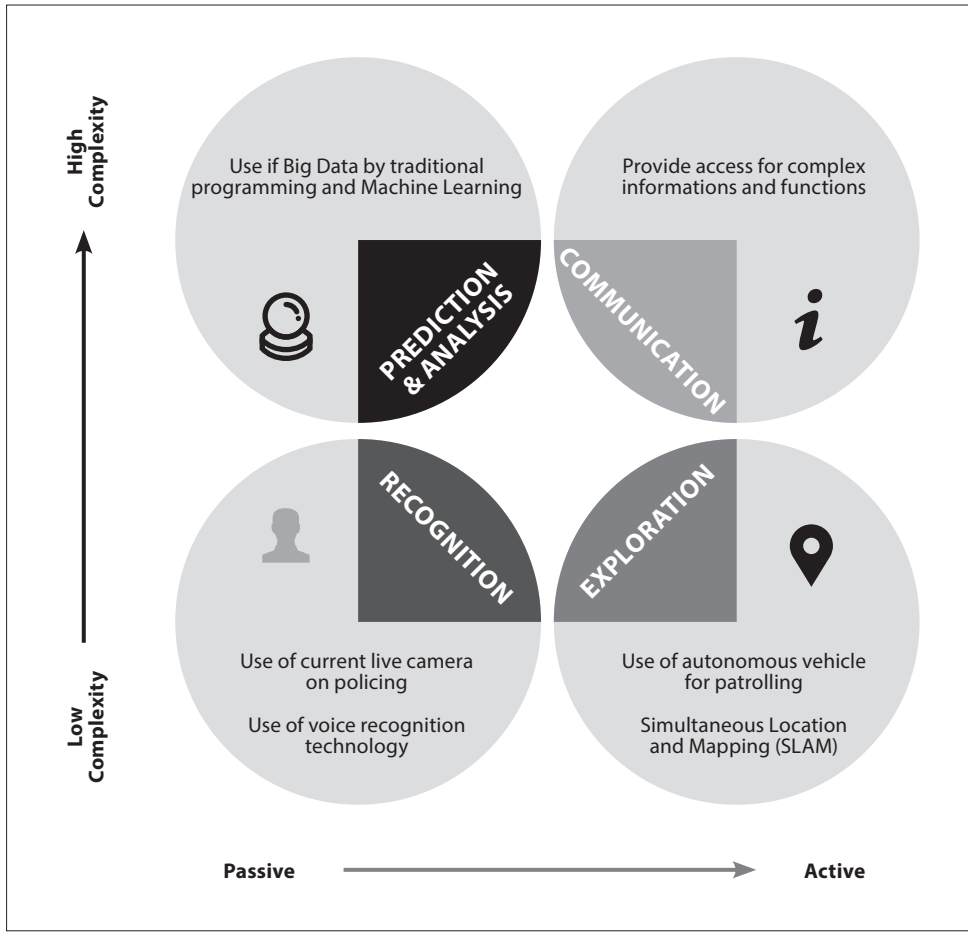

Figure 6 *Artificial Intelligence and Robotics for Law Enforcement (United Nations [UNICRI] Global Meeting on the Opportunities and Risks of Artificial Intelligence and Robotics for Law Enforcement)*

Police, courts, and correctional facilities work in tandem to form the legal criminal justice system. In order to perform at optimal levels, these agencies must have access to experts who are able to analyse crime data and simulate scenarios to enhance precision utilized by Artificial Intelligence programs. One such example is the National Intelligence Model (NIM) in the UK, designed to improve and assist intelligence-led police. NIM consists of nine individual elements:[40]

[39] McCaney, K. "Law Enforcement Using Analytical Tools to Predict Crime". GCN. 22 December 2010. https://gcn.com/articles/2010/12/22/police-predictive-analysis-software.aspx?m=1, Accessed on 22 May 2020.

[40] Alshibly, H., Alzou'bi, S. and Al-Ma'aitah, Mohammed. 2014 "Artificial Intelligence in Law Enforcement, A Review." *International Journal of Advanced Information Technology* 4/4. 2014. 1–9. https://doi.org/10.5121/IJAIT.2014.4401

– Crime Pattern (number/relations);
– Criminal surveys;
– Demographic/ Social Trend Analysis;
– Profiling of criminal operations;
– Network analysis (actors who make up such networks);
– Risk analysis;
– Target profile analysis;
– Operational Intelligence assessment;
– Results analysis evaluating effectiveness of various law enforcement activities.

UNICRI's report concluded that AI and robotics could be weaponized as much as it could be utilized for public good in policing for crime prevention, stating "A recent report by 26 authors from 14 institutions (spanning academia, civil society, and industry) investigated the issue in depth and suggested that many of the same features that might make AI and robotics appealing for law enforcement (such as scale, speed, performance, distance) might make AI and robotics equally appealing for criminals and terrorist groups".[41]

The report identified three main areas of attack:
– Digital attacks like automated spear phishing, automated discovery and exploitation of cyber-vulnerabilities.
– Political attacks, such as the spread of fake news or media to generate confusion, conflict or face-swapping (deep fake) and spoofing tools to manipulate video and create trust issues in political figures or even result in the validity of evidence being questioned in court.
– Physical attacks, such as facial recognition capabilities in armed drones or drones smuggling contraband. In the context of digital attacks, the report further noted that AI could be used either to directly carry out a harmful act or to subvert another AI system by poisoning data sets.[42]

CYBER WARFARE APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN HUNGARY

There had been enough development which had occurred in DLTs and blockchain technology use cases beyond cryptocurrency. It is evident, that these technologies can be combined with other emerging ones, and an examination is required to understand, how the new technologies might be applied in the profession of arms. International research found that the armed forces of the most powerful countries, such as the US, China and Russia have all publicly discussed the military applications of blockchain.[43]

In Hungary, being the gate for the European Union and Schengen zone, there are numerous challenges in monitoring the border. These challenges could be tackled by using distributed network based computer vision detection tools, such as UAVs (drones) for the lengthy border and fence monitoring. The captured images of the UAVs could be automatically

[41] Madhavan, R. "Artificial Intelligence in Policing: Use-Cases, Ethical Concerns, and Trends." EMERJ. 19 December 2016. https://emerj.com/ai-sector-overviews/artificial-intelligence-in-policing/, Accessed on 22 May 2020.

[42] Simerly, M. T., Keenaghan, D. J. "Blockchain for military logistics". *Army Sustainment,* 4 November 2019. https://www.army.mil/article/227943/blockchain_for_military_logistics, Accessed on 22 May 2020.

[43] Bilyana, L. and Sale L. „Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia". *The RUSI Journal* 166/3. 2021. 46–56, DOI: 10.1080/03071847.2021.1886871

classified and analysed using AI algorithms, which would improve the decision makers to send human resource (military) for further investigation of the designated border zone. Illegal migration and border trespassing could be also monitored in an automated way.

Another smart application of the technology would be to monitor the human activity patterns at the borders. Computer vision based Human Activity Recognition (HAR) is therefore a research area for the future, as it could provide relevant information to the authorities about abnormal activities and events.

A crucial feature of such recognition systems in these VUCA (volatile, uncertain, complex and ambiguous) environments[44] is the object detection. For law enforcements, manual video review can take enormous manpower and time, while the human error is at a higher possible rate at these manual reviews. Using a distributed network for secure data storage, and artificial intelligence algorithms to detect different types of objects (with customization options, such as type of object, colour of the object, etc.) the armed forces, police and other units could save significant time because of the improved accuracy of object detection.

CONCLUSION

Blockchain military applications are not combat ready yet, but AI applications are getting much more widespread. Biometrical identifications (face recognition) are used at various industries, so computer vision, machine learning and AI will all go through a revolution. While there are novel suggestions for military applicability of these technologies, so far defence logistics seems to benefit the most from DLTs and blockchain.

According to a research report published by Accenture, "six in seven (86%) aerospace and defence companies plan to integrate blockchain within three years" while "93% of aerospace and defence executives believe that the next generation of intelligent solutions are moving into physical environments".[45] When a nation decides to develop and/or upgrade its cyber security strategies at a federal level, challenges and dilemmas arise as to the concerns examined by specific approaches and policies and how these cyber-challenges will be addressed. Kovács emphasizes the importance of considering the "recommendations made by the international organizations, which can serve as a basis for building a country's national cyber security strategy and its key regulatory issues".[46]

Due to cyber space evolving at such an exponential rate, NATO and the European Union have compiled individual policies regarding cyber security. NATO's conclusions regarding cyber security policies and regulations discuss the interpretation of cyberspace as a domain of warfare, which has many consequences for member states (for example, delegating broader cyber defence tasks to the army, building cyberattack capabilities, setting up cyber commands).

Another aspect of NATO's Cyber Pledge is to approximate the differing levels of cyber defence capabilities per member state. As these levels have significant gaps, NATO's Cyber Operation Centre can play an important role, not only in military but also in the

[44] Jobbágy, Z. "Innovation Methodologies for Defence Challenges: On Design Thinking and Organic Approaches". *Hungarian Defence Review* 148/2. 2020. 50–64. https://doi.org/10.35926/HDR.2020.2.3

[45] "Launchpad to Relevance: Aerospace and Defence Technology Vision 2018". Accenture. 1 June 2018. https://www.accenture.com/_acnmedia/PDF-79/Aerospace-Defence-Tech-Vision-2018.PDF, Accessed on 22 May 2020.

[46] Kovács. "National Cyber Security as the Cornerstone of National Security."

civil defence sector.[47] The Alliance promotes the strengthening of international cooperation between both member states and non-NATO countries in terms of innovative technologies.

Blockchain technology additionally reverses the computer security paradigm. Firstly, it is reliable since both internal and external users must compromise on the network. Second, it is transparently secure and does not rely on malfunctioning nodes, but rather on a cryptographic data structure that renders manipulation extremely complex and immediately apparent. Finally, blockchain networks are fault tolerant, coordinate trusted nodes meaning untrusted entities are rejected. As a result, blockchain networks not only reduce the likelihood of failure, but also significantly increase the cost of attempted breaches by foreign parties.

It is recommended that organic expertise is developed in blockchain technologies within the Central Defence Management Authorities, as well as looking for strong partnerships with the industry to formulate synergies for the development of blockchain-based technologies and the mutual benefits they bring. The Hungarian Defence Forces could adapt artificial intelligence detections at the border protection, at institutional security, and at public safety applications (using existing infrastructure of CCTVs). Further research could go into the application of UAVs and portable optical infrastructures (self-driving cars, such as the ones used for Google Street view). The ever-evolving cyber world requires more stringent regulations and accountabilities. As much as developed nations are trying to grapple with the influx of cyber-related challenges, underdeveloped nations need to prepare as well as each country has a prerogative to protect its people. Blockchain technology and Artificial Intelligence provide the key in developing smarter and more secure cyber defence systems overall.

BIBLIOGRAPHY

- Allen, G. C. "Project Maven Brings AI to the Fight Against ISIS." *Bulletin of the Atomic Scientists,* 21 December 2017. https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/, Accessed on 22 May 2020.
- Alshibly, H., Alzou'bi, S. and Al-Ma'aitah, Mohammed. "Artificial Intelligence in Law Enforcement, A Review." *International Journal of Advanced Information Technology* 4/4. 2014. 1–9. https://doi.org/10.5121/IJAIT.2014.4401
- Andersen, C. "The Great Chain of Being Sure About Things." *The Economist,* 31 Oct 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things, Accessed on 22 May 2020.
- "Arleigh Burke-Class (Aegis) Destroyer". Naval Technology. https://www.naval-technology.com/projects/burke/, Accessed on 20 April 2020.
- Axe, D. "Failure to Communicate: Inside the Army's Doomed Quest for the 'Perfect' Radio." The Center for Public Integrity. 10 January 2012. https://publicintegrity.org/national-security/failure-to-communicate-inside-the-armys-doomed-quest-for-the-perfect-radio/, Accessed on 22 May 2020.
- Babones, S. "Smart 'Blockchain Battleships' Are Right Around the Corner." *The National Interest,* 17 May 2018. https://nationalinterest.org/feature/smart-battleships-are-right-around-the-corner-25872, Accessed on 22 May 2020.

[47] "Cyber Defence". NATO. 17 March 2020. https://www.nato.int/cps/en/natohq/topics_78170.htm, Accessed on 22 May 2020.

- Bilyana, L. and Sale L. „Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia". *The RUSI Journal* 166/3. 2021. 46–56, DOI: 10.1080/03071847.2021.1886871
- Bower, J. L. and Christensen, C. M. "Disruptive Technologies: Catching the Wave." *Harvard Business Review* 73/1. 1995. 43–53. https://hbr.org/1995/01/disruptive-technologies-catching-the-wave
- Bretl, T., Righetti, L. and Madhavan, R. "Epstein, Project Maven, and Some Reasons to Think About Where We Get Our Funding." *IEEE Robotics & Automation* 26/4. 2019. 8–13. DOI: 10.1109/MRA.2019.2943271
- Crofts, P. and Rijswijik, H. v. "Negotiating 'Evil': Google, Project Maven and the Corporate Form." *Law, Technology and Humans* 2/1. 75–90. DOI: 10.5204/lthj.v2i1.1313
- "Cyber Defence". NATO. 17 March 2020. https://www.nato.int/cps/en/natohq/topics_78170.htm, Accessed on 22 May 2020.
- "DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23." United States, Department of Defence. 12 July 2019. https://media.defence.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF, Accessed on 17 April 2020.
- Dwyer, G. P. "The Economics of Bitcoin and Other Private Digital Currencies." *Journal of Financial Stability* 17. 2015. 81–91. DOI: 10.1016/j.jfs.2014.11.006
- Ferdinando, L. "'Terabyte of Death' Cyberattack against DoD Looms, DISA Director Warns". 11 January 2018. https://www.defense.gov/Explore/News/Article/Article/1414146/terabyte-of-death-cyberattack-against-dod-looms-disa-director-warns/, Accessed on 20 April 2020.
- "Galois and Guardtime Federal Awarded $1.8 Million DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System". Galois. 13 September 2016. https://galois.com/news/galois-guardtime-formal-verification/, Accessed on 20 April 2020.
- Garstka, J. J. "Network-Centric Warfare Offers Warfighting Advantage." *SIGNAL Magazine,* May 2003. https://www.afcea.org/content/network-centric-warfare-offers-warfighting-advantage, Accessed on 20 April 2020.
- Haber, S. and Stornetta, W. S. "How to time-stamp a digital document." *Journal of Cryptology* 3/2. 1991. 99–111. DOI: 10.1007/bf00196791
- Haig, Zs. "Connections between Cyber Warfare and Information Operations" *AARMS* 8/2. 2009. 329–337. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1900/13haig.pdf, Accessed on 20 April 2020.
- Hashim, H. "Military Applications of Blockchain Technology." *Fintech News,* 1 July 2020. https://www.fintechnews.org/military-applications-of-blockchain-technology/
- Jobbágy, Z. "Innovation Methodologies for Defence Challenges: On Design Thinking and Organic Approaches". *Hungarian Defence Review* 148/2. 2020. 50–64. https://doi.org/10.35926/HDR.2020.2.3
- Kovács, L. "National Cyber Security as the Cornerstone of National Security." *Land Forces Academy Review* 23/2. 2018. 113–120. DOI: 10.2478/raft-2018-0013
- Kovács, L. "National Cybersecurity Strategy Framework." *AARMS* 18/2. 2019. 65–76. DOI: 10.32565/aarms.2019.2.9
- "Launchpad to Relevance: Aerospace and Defence Technology Vision 2018". Accenture. 1 June 2018. https://www.accenture.com/_acnmedia/PDF-79/Aerospace-Defence-Tech-Vision-2018.PDF, Accessed on 22 May 2020.
- Lindorff, D. "Exclusive: The Pentagon's Massive Accounting Fraud Exposed". *The Nation,* 27 November 2018. https://www.thenation.com/article/archive/pentagon-audit-budget-fraud/, Accessed on 22 May 2020.

- Lindsay, J. M. (host). "Killer Robots and Autonomous Weapons With Paul Scharre". Podcast. 1 June 2018. https://www.cfr.org/podcasts/killer-robots-and-autonomous-weapons-paul-scharre, Accessed on 28 May 2020.
- Madhavan, R. "Artificial Intelligence in Policing: Use-Cases, Ethical Concerns, and Trends." EMERJ. 19 December 2016. https://emerj.com/ai-sector-overviews/artificial-intelligence-in-policing/, Accessed on 22 May 2020.
- Malik, A. A., Mahboob, A., Khan, A. and Zubairi, J. "Application of Cyber Security in Emerging C4ISR Systems." In *Crisis Management: Concepts, Methodologies, Tools, and Applications*. Hershey: Information Science Reference, 2014. 1705–1738. DOI: 10.4018/978-1-4666-4707-7.ch086
- McAbee, A., Tummala, M. and McEachen, J. "Military Intelligence Applications for Blockchain Technology." In *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Honolulu: University of Hawai'i at Mānoa, 2019. DOI: 10.24251/HICSS.2019.726
- McCaney, K. "Law Enforcement Using Analytical Tools to Predict Crime". GCN. 22 December 2010. https://gcn.com/articles/2010/12/22/police-predictive-analysis-software.aspx?m=1, Accessed on 22 May 2020.
- McCarter, J. "DON Innovator Embraces a New Disruptive Technology: Blockchain". Secretary of the Navy. 22 June 2017. https://www.secnav.navy.mil/innovation/Pages/2017/06/BlockChain.aspx, Accessed on 22 May 2020.
- Mire, S. "Blockchain for Military Defence." *Disruptor Daily,* 9 November 2018. https://www.disruptordaily.com/blockchain-use-cases-military-defence/, Accessed on 22 May 2020.
- Nassar, A. R. and Reutzel, E. W. "A proposed digital thread for additive manufacturing". In *Proceedings for the 2013 International Solid Freeform Fabrication Symposium*. Austin: University of Texas, 2013. 19–43. http://utw10945.utweb.utexas.edu/Manuscripts/2013/2013-02-Nassar.pdf
- National Defence Authorization Act for Fiscal Year 2018, H.R. 2810, 115th Cong. (2017–2018)
- Pawlyk, O. "If It's Not Ethical, They Won't Field It: Pentagon Release New A.I. Guidelines". Military.com. 24 February 2020. https://www.military.com/daily-news/2020/02/24/if-its-not-ethical-they-wont-field-it-pentagon-release-new-ai-guidelines.html, Accessed on 23 April 2020.
- Perera, W. "Understanding Blockchain: How it works". *The Capital,* 13 May 2020. https://medium.com/the-capital/understanding-blockchain-how-it-works-5772e29421b8, Accessed on 28 May 2020.
- Pinna, A. and Ruttenberg, W. *Distributed ledger technologies in securities post-trading: revolution or evolution?* Frankfurt: European Central Bank, 2016. DOI: 10.2866/270533
- Popescu, V. A., Popescu, G. and Popescu, C. R. "The amazing world of the Internet-Challenges of the Internet Age". *Manager Journal* 12/1. 2010. 13–23. http://manager.faa.ro/download/536_1202.pdf
- Reed, J. "Israel's Killer Robot Cars". *Foreign Policy,* 20 November 2012. https://foreignpolicy.com/2012/11/20/israels-killer-robot-cars/, Accessed on 28 May 2020.
- Sanchez, S. L. "Blockchain Technology In Defence". *European Defence Matters* 14. 2017. 17. https://www.eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence
- Simerly, M. T. and Keenaghan, D. J. "Blockchain for military logistics". *Army Sustainment,* 4 November 2019. https://www.army.mil/article/227943/blockchain_for_military_logistics, Accessed on 22 May 2020.
- Swan, M. *Blockchain: Blueprint for a New Economy.* Sebastopol, CA: O'Reilly Media, 2015.
- Tapscott, D. and Tapscott A. *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. London: Penguin, 2016.
- Wyden, R. *Ron Wyden to Alan R. Lynn, 22 March 2017.* Letter. https://www.documentcloud.org/documents/3527403-Ron-Wyden-DISA-STARTTLS-Letter-March-22.html, Accessed on 17 April 2020.