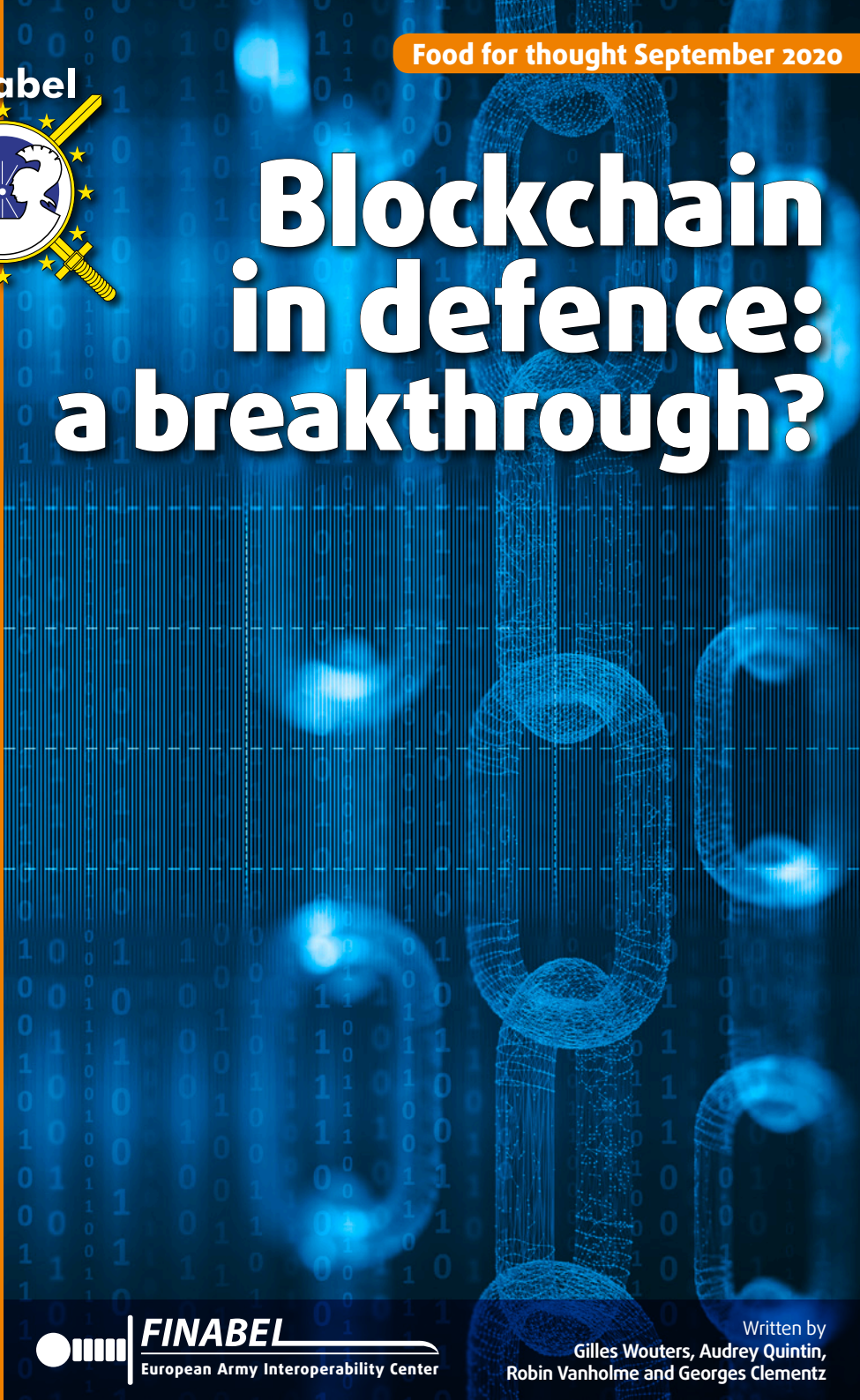
Finabel

Food for thought September 2020

Blockchain in defence: a breakthrough?



AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Center

Written by
Gilles Wouters, Audrey Quintin,
Robin Vanholme and Georges Clementz

This paper was drawn up by Gilles Wouters, Audrey Quintin, Robin Vanholme and Georges Clementz under the supervision and guidance of Mr Mario Blokken, Director of the Permanent Secretariat.

This Food for Thought paper is a document that gives an initial reflection on the theme. The content is not reflecting the positions of the member states but consists of elements that can initiate and feed the discussions and analyses in the domain of the theme. All our studies are available on www.finabel.org

TABLE OF CONTENT

INTRODUCTION

Blockchain is set to radically change our way of life in the coming decades. That is why many authors, like Marc Andreessen, considered it *"one of the most important technologies since the advent of the Internet."* (Finance Train, 2019). Based on a peer-to-peer (P2P) topology, blockchain is a distributed ledger technology that allows data to be stored globally on thousands of servers – while letting anyone on the network see everyone else's entries in near-real-time (ComputerWorld, 2019). In other words, blockchain can be described as a global online database, that anyone, anywhere in the world, with an internet connection, can use. As a consequence, a blockchain doesn't belong to anyone, and it stores information permanently across a network of personal computers. Consequently, it can be seen as a revolutionary technology, thanks to its decentralised nature and its ability to distribute information among its participants, in total transparency evenly.

Blockchain's most popular application is Bitcoin. Allegedly invented by the pseudonymous Satoshi Nakamoto, Bitcoin is a digital currency created and held electronically, which can be sent to anyone, whether or not they are known to the sender. Bitcoin relies on a ledger of transactions much like a bank maintains, but with copies of that ledger distributed among computers all over the world, automatically updating with every transaction. Maintaining this distributed ledger requires a lot of work, but it was no one's job to do this work. Instead, the system pays out cryptocurrency to those who volunteer to do it. This allows for the maintenance of the decentralised ledger – a ledger maintained not by a single party, but by a network of people.

The several advantages of the blockchain (such as its resilience, security and immutability), mostly due to its decentralised nature, make it particularly useful in defence. Indeed, this technology can be used both in operational and support roles, and the private blockchain is privileged in this field. Firstly, blockchain represents a powerful tool to prevent cyber-attacks, whether this is on the battlefield, in intelligence, the defence industry, or government defence departments. Secondly, blockchain technology can assist in managing defence supply chains, which constantly accumulate actors and complexity. Blockchain can ensure the accuracy of identities and improve the traceability of the materials (including sensitive ones like weapons), at each step from their source to their destination.

Consequently, it will offer a better overview of the resources available and reveal inefficiencies. Thirdly, blockchain technology is useful for strengthening the resilience of communications, within armies, departments of defence as well as in the defence industries. Finally, blockchain could also help secure personal data confidentiality, 3D printing data, soldiers registers or smart contracts.

The advent of blockchain technology has caused a particular excitement across businesses and governments. Many researchers remain sceptical about the advantages of blockchain for DoD operations, and some point out that the structure of the technology may impede them. The so-called "immutability" of data in a blockchain is guaranteed as long as the network is big enough and the participation is well distributed among the users. But as we shall see, this isn't always the case, and the defence sector should be aware of it. If a user is infected in a permissionless network (a network which you can join without having to ask for permission), and other users are aware of it, they can easily ignore him and the blocks he is attempting to post. But if data from a permissioned network owner or consortium member is accessed, it will have more severe implications. If the owner or part of the consortium is compromised, so is the network. Blockchain isn't as invulnerable as is often thought, and we shall delve into its challenges and limits regarding its implementation in the defence sector.

In this paper, we will examine how blockchain works and discuss its civilian and military uses. We shall see how numerous departments of defence all over the world are working on implementing blockchain technology for defence and security purposes. This paper shall also address in detail the developments within the main countries and powers that are currently integrating blockchain into their armies, such as China, Russia and the United States. Beyond that, we shall analyse how blockchain, like any other new technology, still has its shortcomings. This leads us to the questions of whether blockchain has the potential to be a real game-changer in military affairs if it has been investigated thoroughly enough, and whether sufficient funds have been allocated to its optimisation.

APPLICATIONS AND FUNCTIONING OF BLOCKCHAIN TECHNOLOGY

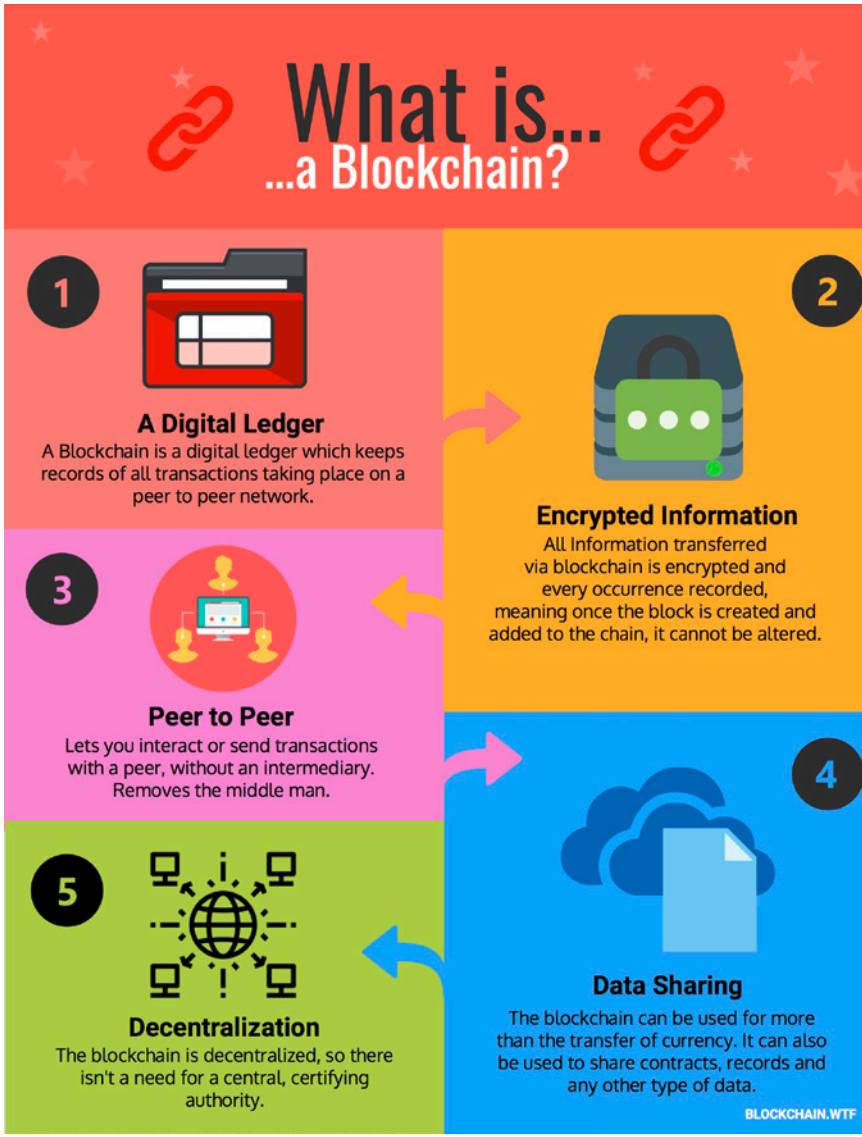
Since its advent in 2008, blockchain has been perceived as a groundbreaking technology. According to Schrepel (2018), a blockchain is "an open and distributed ledger that can record – manually or automatically – all sorts of transactions between users. Once they are recorded, these transactions are permanent and can be seen by all users, which is one of the reasons why blockchain can be trusted. All users agree to a certain set of procedures – called the protocol – which sets the rules of the blockchain. Once the protocol is determined, the blockchain operates under it, and no deviation from it is in theory possible, which creates and enhances trust" (Schrepel, 2018, pp. 288-289). To sum it up, blockchain technology consists of digitally signed and time-stamped data clusters that are published and linked together like a chain. It allows multiple users to post at the same time through a secure algorithm in multiple cyber locations, without the risk of data manipulation. There is only one version of the data, and all users have the same copy that they can separately review. Thus, they can confirm the authenticity of transactions without changing past authenticated data.

Very often, the analogy of a Google Document is used to explain blockchain technology. When we create a document and share it with a group of people, the document is distributed instead of copied or transferred. This creates a decentralised distribution chain that gives everyone access to the document at the same time. No one is locked out awaiting changes from another party, while all modifications to the document are being recorded in real-time, making changes completely transparent.

Regarding its technical functioning, blockchain consists of three important concepts: blocks, nodes and miners. Every chain consists of multiple blocks, and each block has three essential elements: the data in the block; a 32-whole number called a nonce (a nonce is randomly generated when a block is created, and it then generates a block header hash); and a hash, which is a 256-bit number wedded to the nonce. When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined. Mining is the process of adding transactions to the large distributed public ledger of existing transactions.

Another important concept in blockchain technology is decentralisation. No computer or organisation can own the chain. Instead, it is a ledger distributed via the nodes connected to the chain. Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning. Every node has its copy of the blockchain, and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified. Since blockchains are transparent, every action in the ledger can be easily checked and viewed. This is why blockchain is regarded as a trust-based process, with digital signatures and keys to authorise the transactions and identify the participant. Once recorded to a chain, a blockchain cannot be removed nor modified. It can only be added to the chain, which ensures the data's integrity. As a result, blockchain networks not only reduce the probability of compromise but also impose significantly higher costs on an adversary to do so.

In simpler words, all network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that is typical of traditional business networks. No participant can change or tamper with a transaction after it has been recorded to the shared ledger.



(FinDev Gateway; 2018)

As a groundbreaking technology, blockchain has different characteristics. A helpful summary was articulated by Chedrawi and Howeyeck (Saint Joseph University of Beirut Lebanon, 2018). First of all, according to them, blockchains are politically and architecturally decentralised (as no one is controlling them and as they don't possess any infrastructural central point of failure). Therefore, no trust element is needed since no central trusted agency is required. This

characteristic then guarantees privacy and anonymity. Secondly, blockchain technology is distributed, as each participant in the network maintains a complete record of past transactions.

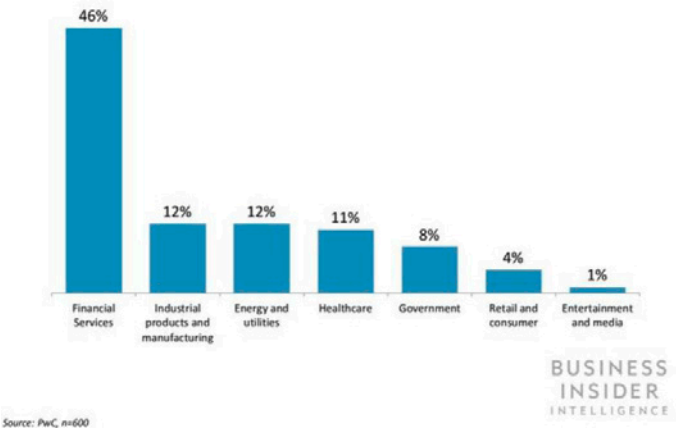
As a consequence, all transactions information is available at any node at any given point in time with equal constitutive value (The Modern Law Review Limited, Paech, 2017). Thirdly, blockchains are disruptive, as they can have a massive impact on any economic or social system. Finally, they are divine, in the sense that identical rules are to be followed in every transaction (Standardised Rules), no modification can be done (Immutability) and no falsification could be made (Persistency).

There are different types of blockchain, which vary from one author to another. According to Buterin (CoinDesk; 2015), they can be roughly categorised into three: public, private and consortium blockchains. A blockchain is public when anyone can read it anywhere in the world. This kind of blockchain is known to be fully decentralised. Conversely, private blockchains, also known as permissioned blockchains, differ from public blockchains in three notable ways. First, participants need permission to join the networks. Second, transactions are private and are only available to ecosystem participants that have been permitted to join the network. Finally, private blockchains are more centralised than public blockchains. Private blockchains are valuable for enterprises that want to collaborate and share data but don't want their sensitive business data visible on a public blockchain. This type of blockchain would seem best suited to be adopted in the defence sector, given the nature and sensitivity of the information generated and stored. Consortium blockchains are sometimes considered a separate designation from private blockchains. The main difference between them is that consortium blockchains are governed by a group rather than a single entity. This approach has all the same benefits of a private blockchain and could be considered a sub-category of private blockchains, as opposed to a separate type of chain. This kind of blockchain can be regarded as partially decentralised because the right to access the network can be limited to a number of participants. Ultimately, we can also evoke the case of permissioned blockchain networks, which can sometimes be used by businesses that want to set up a private blockchain. This places restrictions on who is allowed to participate in the network, and only in certain transactions. Participants need to obtain an invitation or permission to join.

Before discussing the military applications of blockchain technology, it is beneficial to review its other uses. In the last decade, blockchain technology has been steadily gaining traction in traditional business applications around the world, to the point that blockchain-focused venture capital fundraising tripled to $3 billion between the years 2017 and 2018. As already stated before, blockchain has long been associated with cryptocurrency, as it was initially created as the ultra-transparent ledger system for Bitcoin to operate on. However, the technology's transparency and security have seen growing adoption in a number of areas, much of which can be traced back to the development of the Ethereum blockchain. Developed by Vitalik Buterin in late 2013, the Ethereum Project relied on a platform combining traditional blockchain functionality with one key difference: the execution of computer code. Thus, Ethereum blockchain let developers create sophisticated programs that can communicate with one another on the blockchain. Ethereum programmers can create tokens to represent any kind of digital asset, track its ownership and execute its functionality according to a set of programming instructions. Tokens can be music files, contracts, concert tickets or even a patient's medical records. This project has broadened the potential of blockchain to permeate other sectors like media, government and identity security. Thousands of companies are currently researching and developing products

and ecosystems that run entirely on this burgeoning technology.

Industries That Global Executives Believe Are Most Advanced In Blockchain Development



Source: PwC, n=600

As mentioned earlier, one of the primary benefits of blockchain technology is its immutability, which is the unchangeable nature of the "ledger" of data posted to the network. This critical feature can provide widespread benefits across a variety of industries around the world. This is completed by the decentralised aspect of blockchain technology, which is expected to change our life from the way we transact business or manage assets, to the way we use our machines, vote, rent a car and even prove our identity. It will transform banks and other financial institutions, hospitals, companies, and governments, among others. For instance, blockchain can be used to operate decentralised cryptocurrency, as is already the case today. At its simplest, cryptocurrencies, or digital coins, are coins that are passed through an electronic network. To use them, users can make transactions by check, wiring, or cash. Otherwise, one can also use a type of virtual currency, most famously Bitcoin (BTC) but also Litecoin, Peercoin, or Dogecoin, among others, where transactions are made using an electronic coded address.

Furthermore, blockchain technology can be invaluable in the asset management and financial services industries. Recent numbers show that the asset management industry could cut costs by $2.7 billion every year by moving to blockchain technology (Financial Times, 2018). In the financial sector, practical applications of blockchain include client screening and onboarding, record-keeping, data privacy and security, and trade processing. Moreover, blockchain provides a way to securely and efficiently create a tamper-proof log of sensitive activity. This makes it excellent for international payments and money transfers. That is why in 2018, Banco Santander launched the world's first blockchain-based money transfer service. Besides, blockchain-based systems also have the potential to improve capital markets. A McKinsey report identifies three benefits that blockchain solutions offer to capital markets (McKinsey Digital, 2018): faster clearing and settlement; consolidated audit trail; and operational improvements. As traditional financial systems tend to be cumbersome, error-prone and increasingly slow, users find the blockchain cheaper, more transparent and more effective. Consequently, a growing number of financial services are using this system to introduce innovations, such as smart bonds and smart contracts.

Smart contracts are mainly used within the insurance industry. They are digital documents embedded with an if-this-then-that (IFTTT) code, which gives them self-execution. In real life, an intermediary ensures that all parties follow through on terms. The blockchain not only waives the need for third parties but also

ensures that all ledger participants know the contract details and that contractual terms are implemented automatically once conditions are met. All contracts and claims can be recorded on the blockchain and validated by the network, which would eliminate invalid claims since the blockchain would reject multiple claims on the same accident.

Another potential application of blockchain technology is in supply chain management. Blockchain's immutable ledger makes it well suited to tasks such as real-time tracking of goods as they move and change hands throughout the supply chain. Using a blockchain opens up several options for companies transporting these goods. Moreover, media companies have also started to adopt blockchain technology to eliminate fraud, reduce costs, and even protect the Intellectual Property (IP) rights of content. Nevertheless, one of the most promising uses of blockchain is expected to be in the Internet of Things (IoT). It has been argued that blockchain-enabled IoT devices would operate faster and more securely for both users and businesses, enabling less centralised control over the financial industry, internet usage, and ownership rights (Visual Capitalist, 2019). According to Gartner (2019), 20.4 billion IoT-connected devices will be active by the end of 2020, with some estimates showing the IoT market will reach $3 trillion annually by 2026. Thus, blockchain could be used in smart property applications and smart appliances. Finally, the blockchain government, intimately linked to blockchain identity, could also have a significant impact on citizens' lives. National, state, and local governments are responsible for maintaining individuals' records such as birth and death dates, marital status, or property transfers. Yet managing this data can be difficult, especially as most of these records only exist in paper form.

Moreover, citizens have to physically go to their local government offices to make changes, which is time-consuming, unnecessary and frustrating. Blockchain technology could simplify this record-keeping and make the data far more secure. Moreover, blockchain could protect an individual's identity by encrypting it and securing it from spammers and marketing schemes.

The advantages of the blockchain make it particularly useful in defence. This technology can be used both in operational and support roles, and the private blockchain is privileged in this field. Blockchain represents a powerful tool to prevent cyber-attacks, whether this is on the battlefield, in intelligence, the defence industry or the departments of defence.

All of these innovations permitted by the use of blockchain might seem like something out of science-fiction, but they are fast becoming a reality. However, if grounded upon ethical standards, blockchain could become a powerful tool for improving business, conducting fair trade, democratising the global economy, and helping to support more open and equitable societies.

Military uses of the blockchain

Blockchain would be particularly useful in defence. This technology has several advantages that stem from its decentralised nature. Firstly, the distributed structure of the blockchain ensures its availability. It also makes this technology less expensive. Secondly, its resilience, security and immutability are particularly useful to store the data and are a strong asset for many military applications. That is the reason why aerospace and defence industry executives surveyed by Accenture in 2017 (blockchain in Aerospace and Defence, 2017) cited blockchain as one of the top emerging technologies they wanted to promote to increase industry growth and efficiency. Also, defence departments all over the world are increasingly attracted by the power of the blockchain. And, according to European Defence Matters (14th edition, 2017), "in the

coming years, the defence research community is expected to search for new applications for the military based on blockchain technology with predominant candidate areas such as cyber defence, secure messaging, resilient communications, logistics support and the networking of the defence Internet of Things."

Blockchain technology has many utilities in the defence sector, as it can be used both in operational and support roles. In this section, we will mainly focus on the three kinds of uses highlighted by Barnas (2016): cyber defence and data integrity, supply chain management, and resilient communications.

Technically, in the field of defence, it seems that the private blockchain would be the most useful. With a public blockchain, access to the chain would not be controlled, which could be dangerous to protect sensitive information. Since private blockchains are characterised by barriers to entry, with one administration in charge of accepting the participants and defining the rules of the chains (read and write permissions), they are the most suited to defence uses. Access and system rules could be controlled by one entity: the Army Chief. In a context of inter-services governance, a hybrid blockchain would also be possible.

Cyber defence and data integrity

The many benefits of blockchain make it a powerful prevention tool against cyber-attacks and explain why this technology is helpful in several fields linked with cyber defence.

In 2017, 235 GB of classified information belonging to South Korean and American intelligence services were stolen by North Korea. The same year, the European Commission stated that "there were more than 4,000 ransomware attacks per day and 80% of European companies experienced at least one cybersecurity incident. The economic impact of cyber-crime has risen fivefold over the past four years alone" (European Commission, State of the Union, 2017). The US federal government has been the target of more than 60,000 cyberattacks, notably in the energy sector, which is made vulnerable by its connectedness and dependence on computing technology (Mire, 2018). Storing large amounts of highly sensitive information in the same place is particularly risky. It can lead to the "terabyte of death", an expression used to describe the theft of massive classified information by foreign actors. In this context, the resilience offered by the blockchain, with its distributed nature and its ability to detect and block any penetrative attempt, can be significantly helpful.

On the battlefield, soldiers need to be sure that the orders and information they receive are valid and accurate. A centralised entity in charge of digital communication is more vulnerable to attacks that can result in the communication being intercepted or altered. Additionally, if a part of a network is affected, the integrity of the system is not promised, and the whole network can collapse. Once again, blockchain appears as a solution to this challenge. By sharing data horizontally, it democratises the battlespace and establishes a secure environment within which the failure of one node will not imply the failure of the others.

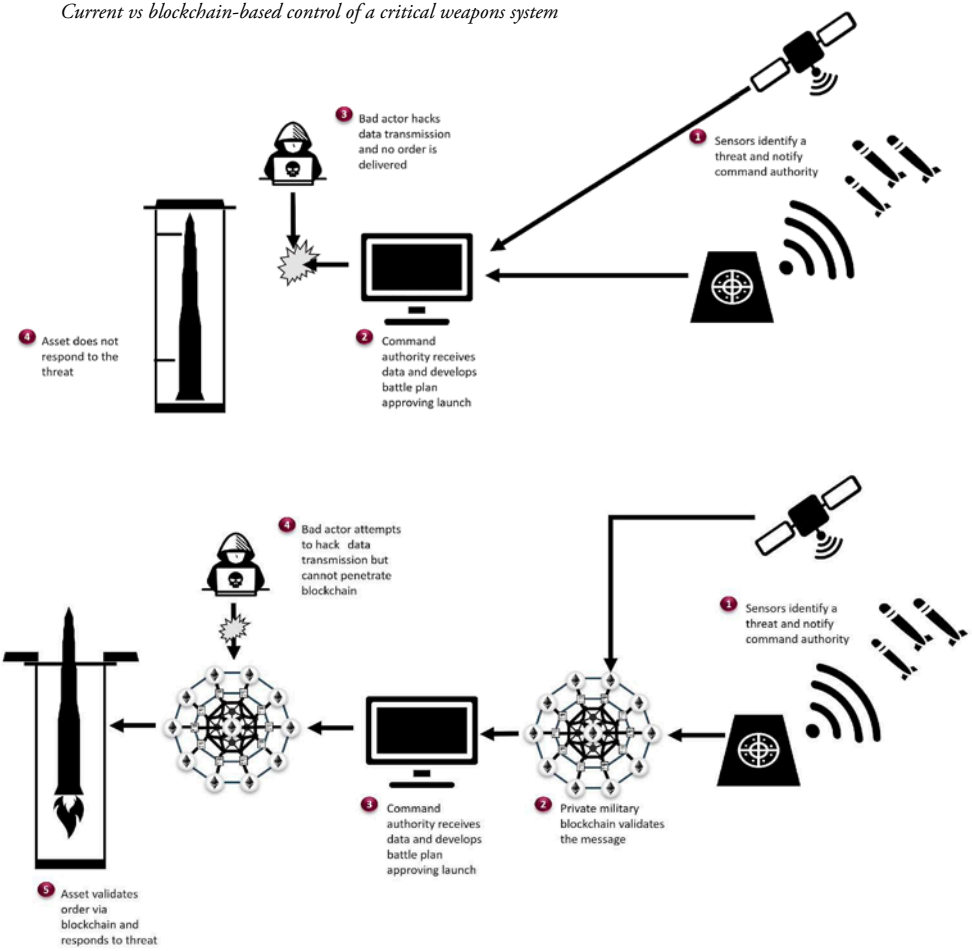
As regards critical weapon systems, traditional weaponry is increasingly combined with the digitalisation of the military. For instance, the US Navy is working on improving the ageing Aegis Combat System by using blockchain to secure more effectively the centralised command-and-control system that links the sensors with weapons within the system. This would enable the weapon to detect targets and fire in under a millisecond (Babones, 2018).

Many actors in the defence industry are eager to rely on blockchain, which gives a single, shared and immutable source of truth. As another report

by Accenture points out (Schmidt, Gelle, and Wheless, 2018), "inaccurate, manipulated, or biased data can have far-reaching, adverse consequences, such as corrupted business insights and skewed decisions". That explains why, according to the report, 86% of aerospace and defence firms in Europe and the US plan to integrate the blockchain technology by 2021. The security of their transactions and supply chains would be strengthened. The collective and decentralised decision-making approach protects these processes from cyberattacks. Blockchains are indeed secure and not alterable thanks to advanced cryptographic techniques.

Technically, these different fields can take advantage of the data integrity permitted by blockchain. Insofar as the blocks cannot be modified without the consent of all the participants or the administration of the chain, data transmissions

Current vs blockchain-based control of a critical weapons system



Source: https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619

are ensured and must come from legitimate actors. Moreover, the security guaranteed by blockchain is not based on secrets or trust, and there are no passwords or cryptographic keys to protect. Finally, the blockchain harnesses the aggregate power of the whole network to resist the attempts of malicious actors actively.

Supply chain management

Currently, military logistics and supply chains gather hundreds of different military and private sector actors. This environment is increasingly complex due to partnerships with developers, start-ups and industry players. Therefore, with so many participants, friction points become unavoidable. That leads to unnecessary costs, inaccuracies or failure points. Yet, blockchain can address these challenges. Regarding military logistics, it offers various advantages: higher delivery speed, traceability, safety, and reduced costs.

One of the most important uses of the blockchain in supply chains is making them more transparent, secure and efficient. First, the verification of the identities is a key element in the defence sector whenever critical weapons and systems are at stake. According to McDonald (2019), "the blockchain can verify that all partners in a defence or aerospace supply chain are operating within established parameters and are indeed who they claim to be".

The traceability of the parts and material used in the defence industry is also crucial. Blockchain technology can help to determine the origin of the weapons from production to delivery and to prevent counterfeits. The date-stamped nature of the blockchain enables users to track past transactions easily. "This is achieved by embedding sensors, reporting processes, and Internet of Things technologies at every step to monitor and report where its materials were sourced from, when and where it was manufactured, how it was transported and stored, and any repairs or maintenance that it has undergone," McDonald explains. Finally, defence companies could combine blockchain technology with others such as artificial intelligence, quantum computing, and extended reality, as a way to boost both data exchanges and data analysis.

The integration of the blockchain at every step of the manufacturing process, including design, prototyping, testing and production, would offer a secured supply chain. The goods could be scanned at each step, giving Departments of Defence logistics teams an overview of the products paths. Currently, the lack of such visibility leads to confusion and miscommunication among supply chain participants, as well as a lack of trust between them (McPherson, Escaravage, Boozallen, no date). By contrast, with blockchain, the private key used by a supply chain partner will enable this partner to be identified. Sensitive information like the type of goods, origin and destination could be encrypted and visible only to allowed participants. Some companies have already chosen the blockchain for this type of use. For instance, in 2018, Accenture and Thales developed a system based on this technology, securing and rationalising the supply chains in the aeronautic and defence sectors. If a piece is dysfunctional, its entrance into the chain and its path may be discovered more quickly thanks to blockchain.

Moreover, while defence systems increasingly use commercial-off-the-shelf components for their software systems, there is growing anxiety that these components could contain deliberate vulnerabilities, exploitable by an adversary whenever it wants (Barnas, 2016). The blockchain could be the solution, establishing the provenance of every processor, circuit board and software component from "cradle to cockpit".

On the battlefields, material traceability and visibility over the product's path are essential. The Army also needs to be confident in pre-positioned materials and movements of capabilities

to succeed in its operations. Blockchain technologies not only permit greater visibility on the material supply chain but can also improve food safety and healthcare on the battlefield. Tracking and tracing the food supply chain can prevent food-related outbreaks and help address the significant issue of the traceability of critical commodities such as pharmaceuticals. Military staff also need to know at each planning level what resources are on hand, in transit or available to request. In other terms, what is required is a near-real-time overview of the material, goods and equipment.

Financial loss and waste are an issue both in the defence industry and during operations. In Afghanistan, for instance, the losses have been estimated to $17 billion for the United States. (Disruptor Daily, 2018). It is crucial to know perfectly where the funds are going and how they will be used. In the Afghanistan example, $2.7 billion of the losses were caused by a dysfunctional air surveillance balloon, and $150 million were wasted on private villas for military staff. The traceability of funds enabled by blockchain would be useful in avoiding such issues in the future.

Resilient communication and other uses

Resilient communications are useful in the Army, notably during operations. It requires, of course, access to the networks during these operations. Also, in a context of high-end conflict, blockchain could provide resilient communications. In this type of conflict, defence departments should be prepared for the enemy to attack the electromagnetic spectrum and, in particular, the critical communication systems such as satellites, undersea cables or tactical datalinks (Barnas, *ibid*). Also, the enemy will try to manipulate data to break the kill chain. To face this threat, armies will need the capability to securely generate, protect and share data, which is possible thanks to chains of blockchain, as explained above.

Furthermore, blockchain could be beneficial to secure messaging systems. Blockchain's cryptographic encryption techniques would permit the implementation of a measure of automation that could reduce the costs and improve both interagency and in-field communications. In line with this, the Defense Advanced Research Projects Agency of the US launched in 2016 a call for tenders for its "Secure Messaging Platform" project whose goal was to transfer messages to a decentralised protocol (Mire, 2018). NATO is also showing a desire to assist its members in implementing blockchain solutions. Because of the geographic emplacement of the members on the two sides of the Atlantic, secured communication is a vital issue, both for the annual meeting and during the interim.

The many advantages of blockchain also make it useful for other applications in the field of defence. First, thanks to this technology, personal data confidentiality could be ensured. A digital identity, stored on the blockchain, could not be falsified. While blockchain has already been used by the UN to help Syrian refugees buy food (WFP, 2020), it could be particularly useful in a defence context to create combatant trackers... These trackers would be distributed between units and searchable by all participants, which would allow for checking the soldiers' real-time location on the battlefield instantly. Second, blockchain offers greater order accuracy through smart contracts. Using them, allies can automatically commit funds to agreed initiatives and shared infrastructure, enhancing supranational defence projects.

Finally, as 3D printing is increasingly used to construct buildings but also to manufacture drones, grenade launchers, body armour and other equipment, blockchain can serve as a more secure transmission tool for data thanks to its distributed nature.

DEVELOPMENTS IN THE BLOCKCHAIN TECHNOLOGY IN THE MILITARY AROUND THE WORLD

Blockchain technology (BT) started to be used in the public sector for the first time in 2012, in Estonia. After a nationwide hack in 2007, the Estonian government decided to heavily invest in secured digital technologies; blockchain was one of these technologies. It was decided to test the applicability of blockchain technology for the registries of the Estonian Ministry of Justice. The technology chosen by Estonian authorities was that of the KSI blockchain. This technology was created by the Estonian tech company Guardtime after years of research and is now used globally. KSI is used for making networks, systems and data secured, fast and efficient, all while retaining total data privacy (PwC, 2019). The technology of KSI significantly increases the cyber safety of data systems. Consequently, the technology developed from KSI is even used by NATO and the US Department of Defense.

For a few years now, numerous states throughout the world have studied how they could develop and introduce blockchain in their security and defence sector. Indeed, over the two coming decades, the US Department of Defense estimates that blockchain will likely dramatically change how the military and its special operations forces operate. The list of countries that have launched initiatives to implement blockchain technology in military applications includes all the major actors: Russia, China, the USA, but also the EU, France, Japan, South Korea, Thailand and Israel. Each one of them hopes to "harness the advantages of this ascending technology" (Willink, 2018). It has long been recognised that cyberspace is the fifth military domain after land, sea, air and space, and as such, the quest for military applications of blockchain has started. This section shall give an overview of which countries are investigating blockchain for military purposes, and where blockchain technologies are under development.

European Union

The European Commission started funding blockchain projects for the first time in 2013. The EU argues that blockchain can impact the foundations of large parts of the EU economy. Currently, the EU is building a European Blockchain Services Infrastructure which will deliver EU-wide cross-border public services using blockchain technology and should be ready this year.

As proof that the EU takes blockchain seriously, it is important to mention that the technology is now one of the priorities of part of the objectives of the Digital Single Market initiative of the EU. Moreover, the Commission now has a dedicated blockchain unit in its Communication and Technology Directorate-General (DG CONNECT).

The EU is financially supporting BT with hundreds of millions of euro (Gabriel, 2018). European Commissioner for Digital Economy and Society, Mariya Gabriel, explained that "we need to boost skills: there are not enough developers, engineers, and blockchain experts. [...] We need to support interoperability and ensure that blockchain can work globally based on international standards" (Marya Gabriel, *ibid*).

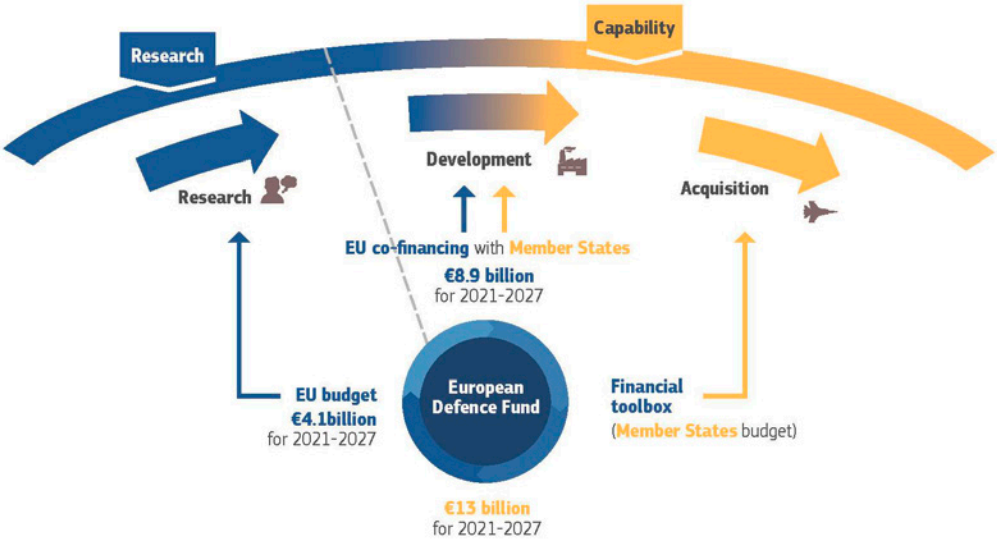
As for the defence sector, from 2021 onwards, the EU will be able to fund eligible companies – and especially SMEs – researching and developing blockchain technology for military applications thanks to the European Defence Fund initiative. The EU's upcoming Horizon Europe support mechanism for science and technology projects should also be able to fund dual-use civilian-military BT systems. Blockchain research should be carried out and funded in the immediate future to improve "cyber defence, secure messaging, resilient

communications, logistics support and the networking of the defence Internet of Things" (EDA, 2017).

For the EU's dedicated defence body – the European Defence Agency (EDA) – blockchain has become a particular topic of interest given its potential use in cyberattacks and cyber-resilience. Among others, information security, authentication, data integrity and resilience are military applications of blockchain being explored by the EDA. However, according to the EDA, the real applications and benefits of BT in the fields of communications and cybersecurity will likely not be seen until 2025 at the earliest (EDA, *ibid*).

In France, last November, Minister of Defence Florence Parly signed a cyber defence convention with eight important defence industrial groups (Airbus, Ariane Group, Dassault Aviation, MBDA, Naval Group, Nexter, Safran et Thalès). The convention aims at enhancing the cyber defence capabilities of the sensitive French defence industries. The goal here is similar to what we can find in South Korea for instance: creating a single online system for the supply chain and procurement process by using blockchain to secure it, as well as making it faster and more efficient.

In Estonia, as mentioned above, the authorities gained first-hand experience in blockchain by creating a huge online platform using the technology. This platform is used by all Estonian citizens, to allow them to see which data the government has on them, as well as to help them communicate with the government. Thanks to this experience with blockchain that other countries do not have, Estonia became host to the NATO Cooperative Cyber Defence Centre of Excellence and the European IT agency. The Estonian blockchain platform provides real-time alerts to cyberattacks, enabling the government to respond to incidents immediately before large-scale damages occur.



Functioning of the European Defence Fund (Source: ASD Europe)

United States

For many countries, digital technologies have transformed warfare. But apart from the US, few have been such pioneers in defence research. Since the 1990s, digital technologies have become the basis of US weapons, tactics, and strategy. Today, soldiers use digital tools and connected devices for almost everything, from airstrikes to spy drones and streaming videos of the battleground. For these purposes, it is crucial to have communications networks that are reliable and secured. Although the US is already able to provide a secure and decentralised data environment for its armed forces, blockchain could further strengthen its management and defence systems. Lately, the US have been very active in the research of military applications for blockchain. In the $700 billion 2019 annual defence budget, blockchain is mentioned by name. This suggests the US military is increasingly interested in BT.

© Shutterstock/Gorodenkoff

In terms of practical applications, the US Defense Advanced Research Projects Agency (DARPA) is working on weaponising blockchain. The main area of concern for DARPA is data integrity systems, meaning ensuring that data are still in their original state, and seeing who has viewed these data. As such, DARPA has launched several projects related to BT to be used in several military domains such as secured hardware systems and quick military logistics. For instance, a few years ago, DARPA created a secured communication network using blockchain (Jakobson, 2019). As for the supply chain processes, which are often hacked to alter or infect data within the process, blockchain is also useful.

Consequently, DARPA is working on using BT to secure the US defence supply chains from cyber-attacks (Hamilton, 2018). Meanwhile, the US Army's Space and Terrestrial Communications Directorate is also turning to blockchain to monitor potential cybersecurity breaches in communications data. Finally, the US DoD is expected to submit this year a highly anticipated report to Congress, demonstrating precisely how blockchain is expected to be incorporated into the US military (Cryptopolitan, 2020).

The leading US defence firm Lockheed Martin is the first American contractor to incorporate blockchain networks into its development processes. Lockheed Martin was awarded a contract to integrate cyber-related elements to processing systems, supply-chain risk management, and software development. The long-time partner of the US military is designing a non-traditional cybersecurity system for the US Department of Defence (DoD) to be used for business transactions with defence and security companies. According to Ron Bessire, Lockheed Martin Aeronautics' Vice President for Engineering and Technology, the intent is to "enhance data integrity, speed problem discovery and mitigation, and reduce the volume of regression testing" (MES, 2017). Incorporating blockchains within the military supply chain will streamline the system by allowing agencies to order only the components they need to enhance procurement and logistic operations. In the meantime, the US Navy is currently experimenting with blockchain technologies. For instance, the US Navy wants to use blockchain to carry

3D-printed submarine hull by the US Navy. (Source: US Department of Energy).

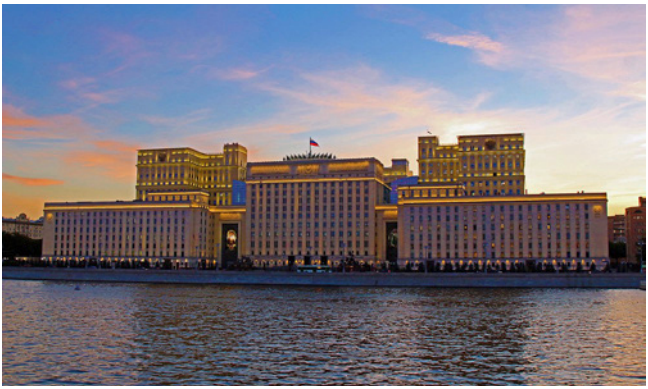
out 3D printing, more specifically, to secure its 3D printing systems. It hopes to resolve some practical and logistical issues by manufacturing military-standard components directly in the field (such as a repair part on a warship at sea).

Russia

The Russian Federation is currently trying to "blockchain" its military communications to make them almost impossible to be intercepted or hacked. To do so, the Russian telecommunication company Voentelecom is working closely with the Russian DoD.

The Russian Ministry of Defence also owns a newly established "Blockchain Research Laboratory", named ERA. This research centre explores how blockchain technology can be used to bolster national security by detecting and preventing hacks on military infrastructure and enhance the military's cyber-security measures (Coindesk, 2016). ERA is also studying investment strategies concerning digital assets and development of technical tasks for the implementation of blockchain technology in corporations and start-ups, all in cooperation with the Russian Financial University. The Russian DoD wants the laboratory to become a technology hub that will, at first, employ about 200 scientists and expects to expand as the technology becomes more important (Coindesk, *ibid*).

According to Maxim Shevchenko, a delegate at the International Standards Organization (ISO), Russia has the "possibility to influence the technology" and to work on the "implementation



The Russian Ministry of Defence building, from where ERA works (Source: Flickr/Emilio)Energy).

[of] Russian standards and solutions worldwide." (NYT, 2018). However, as of now, blockchain technology is currently not mature enough to be used on a mass scale (Chang, 2018). "There is still no big industrial solution on distributed ledgers, except for bitcoins," the Bank of Russia deputy governor Olga Skorobogatov said in 2018 (Chang; 2018). "The technology is not mature enough. It still requires a lot of improvements, both from a security viewpoint and in terms of scalability." Still, this does not prevent ERA from researching how blockchain technology can be used for military applications, to put blockchain into operation in the medium term.

Pragmatically, the Russian Financial Communications Transfer System – created in 2014 as a response to sanctions – adopted blockchain in 2019. This allows Russia to circumvent some of the international financial sanctions against them. Additionally, the Russian Spy Agencies FSB and GRU are financially taking advantage of the blockchain technology related to cryptocurrency. Indeed, it has been reported that Russia owns billions of dollars in cryptocurrencies such as Bitcoin and is taking advantage of the cover provided by cryptocurrency and their exchanges to fund intelligence operations (RFE, 2019).

China

The Chinese private sector has embraced blockchain in their business. A survey by Deloitte (Consensys, 2019) revealed that while more than 90 per cent of Chinese executives said they had or planned to have blockchain solutions in production this year, only 34 per cent of American executives reported similar plans. Similarly, there has been substantial interest within the Chinese DoD to find military purposes for blockchain (Deloitte, 2018).

This substantial interest can now be found at the highest level of Chinese authorities. In 2019, Chinese President Xi Jinping himself called on his country's tech community to accelerate blockchain developments to make it a core part of Chinese technologies across various industrial domains, including the defence sector. Ever since Xi publicly supported blockchain and called it breakthrough technology, government authorities, corporates and state media have invested a lot of time, money and research in blockchain and its applications. Moreover, China is almost ready to launch its national digital currency after five years of research and development (Browne, 2019). Experts and NATO project that China is going to take the lead in blockchain technologies (Barberini, 2020).

Similarly to Russia, it has also been argued that China's defence and security agencies are leveraging blockchain to manage the distribution of funds for intelligence operations. Moreover, China could use blockchain to protect sensitive personnel and weapons data from cyber-attacks and make logistics operations safer and more efficient. According to the country's official army newspaper, the PLA Daily, the Chinese military should use blockchain technology to improve online operations, store military data, and reward soldiers' good performance with online tokens (The Block Crypto; 2019). Military use of blockchain by China could consist of four elements: securing battlefield information, managing weapons and equipment, enhancing military logistics, and facilitating covert intelligence operations.

In conclusion, the development of blockchain in China is well underway. More than 500 blockchain projects have been registered with the Cyber Administration of China (Kharpal, 2019). Considering China's financial capabilities and high interest, there is a chance that China – in the absence of competition from other regions – will have a significant influence or even control over the development of this new technology (Kharpal, *ibid*).

South Korea

South Korea also shows interest in the use of BT in its national defence. For instance, a blockchain authentication solution developed by a private South Korean company is being adopted by the nation's military (Cryptonews, 2020). This company has developed a decentralised ID platform that makes use of blockchain innovations via a mobile app to process biometric information safely. The project has been conducted in conjunction with the Military Manpower Administration, a Ministry of Defence agency.

In 2019, South Korea's state Defence Acquisition Program Administration (DAPA) announced that it is working with multiple other agencies for an interoperable blockchain system. The South Korean arms procurement department wishes to create a more transparent and fairer platform for military administration. The plan is to use blockchain in defence procurement to track efficiently, easily and in an open way all the bidding processes, all the way from the receipt of defence systems proposals to the evaluation of defence contracts. Ultimately, this should reduce the risk of fraud because of the transparency that blockchain provides. The rise of administrative efficiency is another objective as blockchain would implement one single system between everyone. As such, South Korea's military funding programs will also use blockchain (Ledger Insights, 2019).

Additionally, South Korea is introducing blockchain technology to protect private defence actors, such as arms companies. The goal is to make business operations with them more secured. Korean telecom firms are taking this occasion to propose blockchain technology for the military. For example, in 2019, South Korea's largest telecoms firm, KT, announced a blockchain-based security service for connected devices via satellite (Wood, 2019). By gaining expertise in this area, the company hopes to get a deal with the Korean DoD to apply

their blockchain technology in the military, for secured communication services or to develop safe remote access to naval assets.

Thailand

Recently, Thailand has emerged as Southeast Asia's blockchain hub, following a grand strategy and legal framework put in place by its government in this cutting-edge field (Chandler, 2018). And the military sector has not been left behind. Indeed, in 2019, the Thai government signed a contract with Guardtime, the Estonian company that created KSI technologies, to nationally implement blockchain, including for its military. To do so, the Defence Technology Institute (DTI) of Thailand has partnered with Guardtime to provide cyber defence capabilities to the Thai armed forces (Guardtime, 2019).

Specifically, DTI and Guardtime have started a blockchain research program to implement cybersecurity training and a cyber exercise program. Concerning the partnership with Guardtime, Thai Air Chief Marshal Preecha Pradabmook said:

> "DTI has committed itself to be a centre of excellence in Cyber Security Technology, contributing to secure the Royal Thai Armed Forces' weapons system platforms. This collaboration with Guardtime will be the first significant step for DTI in the achievement of Cyber Security Capability" (Guardtime, *ibid*).

Finally, NATO is also researching military-grade blockchain applications. In 2016, NATO's Communications and Information Agency called for blockchain applications regarding military logistics, procurement, and finance as well as "other applications of interest to the military" (NCIA, 2016). Blockchain could also be useful to ensure and facilitate the logistics of NATO information sharing and collaborative procurements between its participating member states, as well as external actors. Finally, NATO, like most public actors involved in blockchain technology for their military, is also looking towards blockchain to secure its communications.

CHALLENGES AND LIMITATIONS OF BLOCKCHAIN: COSTS ASSOCIATED WITH THE TECHNOLOGY, SECURITY LOOPHOLES

> Arthur C. Clarke once wrote, "Any sufficiently advanced technology is indistinguishable from magic". Clarke's statement is a perfect representation for the emerging applications of blockchain technology. There is 'hype' around the use of blockchain technology, yet the technology is not well understood. It is not magical; it will not solve all problems. As with all new technology, there is a tendency to want to apply it to every sector in every way imaginable.
>
> (Yaga et al., 2018, p. iv)

The emergence of blockchain technology triggered a particular frenzy among businesses and governments. Every organisation tried to make use of the new technology that was described as groundbreaking (Beck & Müller-Bloch, 2014). This reached the point where a playbook on blockchain technology had to be written for the US Federal Government to help legislators and administrative bodies navigate these new, uncharted waters (ACT-IAC, 2018). Organisations throughout the globe need to assess where the technology could be implemented. As Yaga et al. (2018, p. vi) put it, we should ask ourselves "how could the blockchain technology potentially benefit us?" rather than "how can we make our problem fit into the blockchain technology paradigm?". A lousy approach can result in faulty implementation, which could increase security risks, whereas a different approach could have mitigated them. In this section, we shall address the various challenges, risks and limitations of blockchain technology. Our primary focus will be on permissioned networks since the military mostly functions with a clear and established chain of command. Permissioned blockchain networks also function through decentralisation, a concept which "is contrary to the traditional military structure that is inherently hierarchical" (Linkov et al., 2018). Implementing this new technology requires a careful approach to avoid disrupting DoD operations which require a rapid response to ever-changing conditions. Linkov et al. remain sceptical about the advantages of blockchain technology to DoD operations. They believe that the structure of the technology may impede the rapid patching of multiple nodes of the network.

Moreover, they explain, "network-wide transparency, which is an important benefit in civilian applications, can become a concern when

sensitive information is transmitted. Proper controls and access must be built into the network to ensure only those with proper credentials can access and update the blockchain" (*ibid.*). McAbee et al. insist that "the key mandatory quality we have identified ... is that the process must be collaborative in nature, which many of the authors filed under shared control" (McAbee, Tummala, McEachen, 2019, p. 6035), a type of control that isn't well suited to the classical top-down communication.

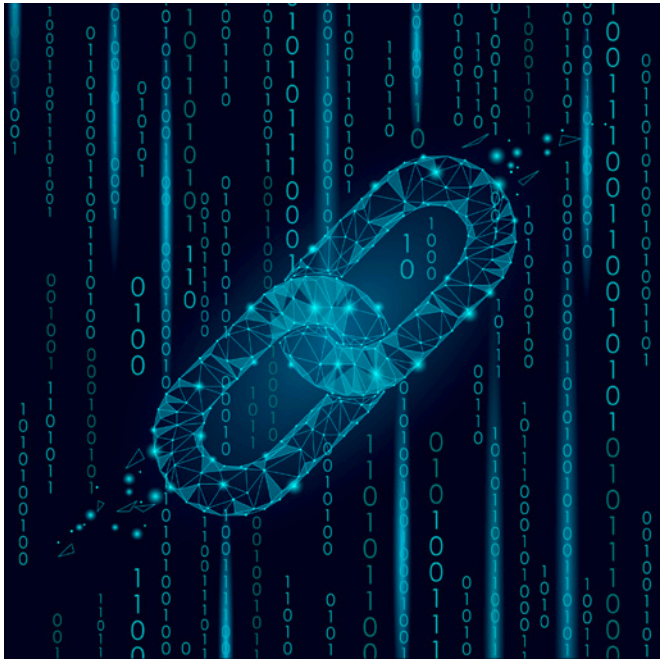
A permissioned network helps avoid or mitigate specific risks, but also creates other problems. Contrary to popular opinion, blockchain networks and their users have not become immune to cyber-attacks. One of the attacks that often occur in permissionless networks is known as the "51% attack". Although information saved on a blockchain is considered nearly impossible to tamper with, such presumed immutability has flaws. To put it simply, the immutability of data in a blockchain is guaranteed as long as the network is big enough, and the participation is well distributed among the users. If a malicious user or group of users gains control of more than 50% of a network's computing power, they can modify certain things in the blockchain. This is possible because users of a network will mostly choose the blockchain with the most extended history. However, permissioned blockchains can help mitigate this sort of attack through the powers allocated to administrators. They can easily remove members entirely, or simply revoke the privileges of any non-cooperating publishing nodes. They control who joins the network as well as the legal aspects that govern the functioning of the blockchain network. But this fact underlines a particular weakness in permissioned networks: their cornerstone is the owner or the consortium in power. In a permissionless network, if a user is compromised and other users become aware of it, they can simply ignore him and the blocks he tries to publish. By contrast, if a permissioned network owner's or consortium member's data is accessed, the consequences will be much direr. Worse, if the owner or part of the consortium is compromised, so is the permissioned network. Possessing access keys and owning content are synonymous in the field of blockchain. Because hackers know that they cannot determine the keys themselves, they spend most of their efforts on stealing them. The weakest point of the entire system is the applications making use of a blockchain, a user's personal computer and their mobile device, which are therefore the best chance to get the desired keys. Cybersecurity risks come not only from systems, network and material, but they also come from human actors. A strong cybersecurity system is therefore essential for securing both the network, its users and participating organisations.

Another important issue stems from blockchain networks' interactions with the real world. A blockchain network can capture real-world input data from both sensors and human actors. Still, so far, no established mechanism can be used to decide whether the input data provides real or corrupt information. A sensor may be faulty and malfunction while recording data. Human actors could intentionally or unintentionally provide false information. Such issues are not exclusive to blockchain networks but are common in digital systems. This is known as the *Oracle problem*, a type of which is referred to as off-chain breaches. Oracles are trusted third parties that connect Smart Contracts with the outside world. They represent a severe flaw within what was thought to be a technology that eliminated the risks of a single point of failure and provided the opportunity to interact on a trustless basis. Now, the importance of trustless relations mainly pertains to permissionless networks. Indeed, the system's anonymity is of vital significance and guaranteed to a certain degree in a permissionless network. As such, the Oracle problem mainly concerns permissionless networks, but it holds crucial warnings for permissioned ones. Information should always be double-checked, especially in permissioned

blockchain systems where users, for one reason or another, should be rendered anonymous.

Therefore, we underline the fact that the emergence of the blockchain does not remove the need for thoughtful and proactive risk management and cybersecurity program. Current programs remain relevant and provide essential safeguards against cyberattacks, but they will have to be adjusted to remain suited to systems that interact with blockchain networks.

Cyber-attacks may compromise the privacy, authenticity and transparency of data recorded in a blockchain. There are omnipresent technological security vulnerabilities that hackers can exploit to cause loss or damage. No proof has been submitted that, for blockchain applications, this would any be different. On-chain breaches can occur in this type of network if a person gains access to it. There are, in this case, two main types of attacks. The first, known as *sybil attacks*, occurs when someone creates a false identity or gains access to credentials to get into the blockchain, to access the data in the blockchain. Another type of issue is that of *man-in-the-middle* attacks, which involve the interception and tampering of encrypted data between two users by a malicious user. In the case of a blockchain network, a malicious user could intercept transactions, redirect them and/or create false ones. Most of these attacks are often carried not on the blockchain network itself, but on the applications that surround it. When developing an application making use of blockchain networks, one has to bear in mind that these same applications are not immune to malicious actors, "who can conduct network scanning and reconnaissance to discover and exploit vulnerabilities" (Yaga et al., 2018, p. 37). This is worrying, especially when considering that new cyber incident response strategies often proved to be inadequate and failed to address the core issues. Such outdated approaches could delay the transition to blockchain technology because personnel would then need to be trained to make full use of its possibilities (Filip Caron, 2017). Innovations in blockchain technology emerge every other week, while hackers garner more and more knowledge about blockchain systems and their vulnerabilities. Most of the qualities attributed to blockchain technologies – such as being secure because of a tamper-evident and tamper-resistant design – are only valid "for transactions which have been included in a published block. Transactions that have not yet been included in a published block within



the blockchain are vulnerable to several types of attacks" (Yaga et al., *ibid.*). For example, time can be spoofed, as members' clocks can be altered to delay communications. Additionally, denial of service attacks can be performed on the blockchain platform to considerably slow down the speed at which the blockchain processes new blocks.

In short, while blockchains provide security and resource advantages, the platform may seem impractical concerning command and control practices. The design, management and technical limits associated with the current blockchains demonstrate these difficulties. For example, blockchains frequently require system updates, which forces users to update their ledger in conjunction with the more extensive system, consuming time and restraining communication for a while. Aside from the security issues discussed earlier, the three main areas of concern surrounding the use of blockchain technology are its scalability, interoperability and environmental sustainability. The scalability refers to the ability of the network to adapt itself to smaller or larger operations, which necessitate different processing speeds. The more information needs to be processed, the more processing power you need. Current blockchain networks lack this processing power. The scalability issue is thus a major flaw in blockchain technology. Another weakness lies in its interoperability: different blockchain networks do not work in the same way, meaning data often cannot be transferred from one network to another due to their fundamental differences. Finally, blockchain networks have often been criticised for their enormous environmental footprint.

Furthermore, the development of blockchain technology implies constant and significant growth in any defence budget. Developing, protecting and controlling such new technology necessitates long-term management and budget planning for the implementation of blockchain to be fruitful.

Adopting and implementing decentralised ledger technologies may be considerably expensive (see e.g. Deshpande et al., 2017). In certain cases, departments with "large existing back-office processes, complex legacy IT systems, or processes created to comply with existing standards (...) could require costly redesign" (Deshpande et al., 2017, p. 8). What's more, not all processes are fit for a blockchain redesign and would require a long-term and profound transformation whose cost-benefit efficiency is unclear.

But Deshpande et al. raise another strong point in terms of prospective challenges and opportunities, which is the elaboration and adoption of common standards for blockchain. Regarding the defence sector, there are multiple potential applications for blockchain. Standards could thus "play an important role in ensuring interoperability between multiple DLT/Blockchain implementations and, in doing so, could help reduce the risk of a fragmented ecosystem" (Deshpande et al. 2017, p. 16). But the elaboration of standards is by itself no small task, especially if different departments are to work together. This task in itself could take years since certain experts cited in the document (anonymised for security reasons), believe that "once the technology is more mainstream and a better understanding of its strengths and weaknesses emerges, the priorities for standards will become clearer" (*ibid.*, p. 20). Blockchain technology first needs to mature before we can assess some form of standards; otherwise, the standards could become quickly outdated and hinder the technology rather than providing a relevant framework. In short, "there is limited consensus on the potential for standards on technical aspects (e.g. format in which data is stored, size of blocks, communications protocols) and their impact on DLT/Blockchain adoption. (...) Further clarity [and time] is needed on the overall technological landscape needed before a stronger case for standards emerges" (*ibid.*, p. 19).

CONCLUSIONS AND RECOMMENDATIONS

As discussed before, blockchain technology has the potential to radically change our way of life, and the way we conduct military operations, both on an operational and support level. Thanks to its decentralised and transparent nature, it could improve the decisions taken by military officials, while enhancing outcomes for military deployments. The development of blockchain technology offers increased data confidence and data availability that can help shape future military logistics and planning. As we saw, the US intends to use it for secured databases, logistics and 3D printing, similarly to China and Russia. The EU is also eager to invest in blockchain and will have the possibility to directly fund blockchain technology related to military fields thanks to the upcoming Horizon Europe framework and the European Defence Fund.

So, is blockchain in the military an evolution or a revolution? An evolution would simply modify how the current military tools are used, while a revolution would dramatically change the tools themselves. Realistically speaking, at present, the evidence suggests an evolution, but not yet a "Revolution in Military Affairs" scale seachange. Blockchain will make communications more secure and facilitate military logistics. Henceforth, blockchain will strengthen and make armed forces more efficient. In the long term, blockchain in the military will be a revolution if it is well implemented and many more military applications are found, in addition to being used wisely and at affordable costs. Still, right now, we are instead witnessing a significant evolution than a real revolution of how armed forces and national DoD operate. Slowly but surely, we can agree that blockchain is becoming a game-changer for the security and efficiency of current military tools, especially if the biggest military actors start implementing it widely; as we saw above, the race between state actors in this field has already begun.

To witness a revolution, blockchain will have to be implemented in most – if not all – defence sectors. To achieve this and to understand the range of blockchain technologies for tactical sustainment challenges, the military should closely examine the potential of blockchain solutions to the challenges associated with in-transit visibility, data integrity, additive manufacturing, large 3D printing, reporting, operational contracting, and logistic estimation, among others. The future shall tell us the real impact of this nascent technology.

BIBLIOGRAPHY

Scientific Articles

- Beck, R; Müller-Bloch, C. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers. Proceedings of the 50th Hawaii International Conference on System Sciences. pp. 5390-5399. Available at: https://pdfs.semanticscholar.org/cdc3/a80f5c77270bd36f1a0212bccea8651de3d4.pdf
- Caron, F. (2017). Blockchain: Identifying risk on the road to distributed ledgers, *Isaca Journal*. Vol. 5.
- Fitzi, M., Gazi, P., Kiayias, A., & Russell, A. (2018). Parallel Chains: Improving Throughput and Latency of blockchain Protocols via Parallel Composition. *IACR Cryptology ePrint Archive*, 2018, 1119.
- Linkov, I.; Wells, E.; Trump, B.; Collier, Z.; Goerger, S.; Lambert, J. (2018). Blockchain Benefits and Risks. Military Engineer. 110.
- McAbee, A. S. M.; Tummala, M.; McEachen, J. C. (2019), "Military Intelligence Applications for blockchain Technology", *Proceedings of the 52nd Hawaii International Conference on System Sciences*. pp. 6031-6040.
- Schrepel, T. (2018). "Is blockchain the Death of Antitrust Law? The blockchain Antitrust Paradox", *Georgetown Law Technology Review*, Vol. 3, N°281, June 11, 2018, available at: https://ssrn.com/abstract=3193576 [last accessed on 16/03/2020].

Press Articles

- Abernethy, M. (2017). "Blockchain becoming an integral part of some defence technology", *Financial Review*, published on July 14th, 2017, accessible at: https://www.afr.com/companies/blockchain-becoming-an-integral-part-of-some-defence-technology-20170713-gxaipa.
- Adams, V. (2019). "Is the US Losing the Race for Web 3.0? ", *ConsenSys Media*, published on February 6, 2019, accessible at: https://media.consensys.net/is-the-u-s-losing-the-race-for-web-3-0-739789dc1ae1.
- Babones, S. (2018), "Smart 'Blockchain Battleships' Are Right Around the Corner", The National Interest, May 17, 2018, available at: https://nationalinterest.org/feature/smart-battleships-are-right-around-the-corner-25872. [last accessed on 14/05/2020].
- Brig. Gen. Mark T. Simerly and Daniel J. Keenaghan. (2019). "Blockchain for military logistics", *The United States Army,* published on October 1st, 2019, accessible at: https://www.army.mil/article/227943/blockchain_for_military_logistics.
- Browne, R. (2019), "China's central bank says it's close to releasing its own digital currency", *CNBC*, August 12, 2019, available at: https://www.cnbc.com/2019/08/12/china-central-bank-close-to-releasing-digital-currency-pboc-official.html [last accessed on 13/05/2020].
- Chandle, S. (2018). "Thailand Proves Crypto Can Win Adoption Even in Military Dictatorships", *Coin Telegraph*, published on November 23, 2018, accessible at: https://cointelegraph.com/news/thailand-proves-crypto-can-win-adoption-even-in-military-dictatorships
- Chang, S. (2018), "The Russian Military Is Building blockchain Research Lab to Combat Hacks" [online], CCN, published on July 3, 2018, available at: https://www.ccn.com/the-russian-military-is-building-blockchain-research-lab-to-combat-hacks/ [last accessed on 13/03/2020].
- Cheng, E. (2018), "Chinese President Xi Jinping calls blockchain a 'breakthrough' technology" [online], *CNBC*, published on May 30, 2018, available at: https://www.cnbc.com/2018/05/30/chinese-president-xi-jinping-calls-blockchain-a-breakthrough-technology.html [last accessed on 13/03/2020].

- Consulting Canada (2019), "blockchain has promising applications in defence sector, says KPMG" [online], *Consulting.ca*, published on August 19, 2019, available at: https://www.consulting.ca/news/1180/blockchain-has-promising-applications-in-defence-sector-says-kpmg [last accessed on 13/03/2020].
- Daley, S. (2020), "Wallets, hospitals and the Chinese military: 19 examples of blockchain cybersecurity at work" [online], *Built In*, published on January 7, 2020, available at: https://builtin.com/blockchain/blockchain-cybersecurity-uses [last accessed on 13/03/2020].
- Eckel, M. (2019), "How Much Did Russian Spy Agencies Rely On Bitcoin? New Hints In Leaked Recordings" [online], *Radio Free Europe*, published on November 28, 2019, available at: https://www.rferl.org/a/how-much-did-russian-spy-agencies-rely-on-bitcoin-new-hints-in-leaked-recordings-/30297083.html [last accessed on 12/03/2020].
- Gabriel, M. (2019). "Blockchain for Europe", *New Europe*, published on February 26, 2018, accessible at : https://www.neweurope.eu/article/blockchain-for-europe/.
- Hamilton, D. (2018), "DARPA blockchain Programs" [online], *Coin Central*, published on October 1st, 2018, available at https://coincentral.com/darpa-blockchain-programs/, [last accessed on 11/03/2020].
- Hebblethwaite, C. (2017), "Defence blockchain study authorised by Trump" [online], *The Block*, published on on December 13, 2017, available at: https://www.blockchaintechnology-news.com/2017/12/13/defence-blockchain-study-authorised-trump/ [last accessed on 13/03/2020].
- Hobbins, J. (2019), "blockchain in Defence: What are the applications?" [online], *Defence iQ*, published on August 8, 2019, available at: https://www.defenceiq.com/defence-technology/articles/blockchain-in-defence-what-are-the-applications [last accessed on 13/03/2020].
- Jagati, S. (2019). "China Is Pushing Blockchain Adoption, Seizing the Momentum From US", *CoinTelegraph*, published on October 30, 2019, accessible at: https://cointelegraph.com/news/china-is-pushing-blockchain-adoption-seizing-the-momentum-from-us.
- Jakobson, L. (2019), "Defense Department turns to blockchain to secure communications" [online], *Modern Consensus*, published on July 30, 2019, available at: https://modernconsensus.com/technology/defense-department-turns-to-blockchain-to-secure-communications/, [last accessed on 11/03/2020].
- Joshi, M. (2020), "US military may incorporate blockchain in 2020" [online], *Cryptopolitan*, published on January 16, 2020, available at: https://www.cryptopolitan.com/us-military-to-incorporate-blockchain/ [last accessed on 13/03/2020].
- Kharpal, A. (2019). "China looks to become blockchain world leader with Xi Jinping backing", *CNBC*, published on December 15, 2019, accessible at: https://www.cnbc.com/2019/12/16/china-looks-to-become-blockchain-world-leader-with-xi-jinping-backing.html.
- Khatri, Y. (2019), "EU Report: blockchain Adoption Will Be Led by Permissioned Platforms" [online], Coindesk, published on March 12, 2019, available at: https://www.coindesk.com/eu-report-blockchain-adoption-will-be-led-by-permissioned-platforms [last accessed on 13/03/2020].
- Llopis Sanchez, S. (2019). "Blockchain technology in defence", *European Defence Matters*, published in 2019, accessible at: https://www.eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence.
- Martin, R. (2018). "5 Blockchain Security Risks and How to Reduce Them", *Ignite*, published on November 29, 2018 and accessible at : https://igniteoutsourcing.com/blockchain/blockchain-security-vulnerabilities-risks/.
- Mire, S. (2018). "Blockchain For Military Defense: 7 Possible Use Cases -", *Disruptor*

Daily, published on November 9, 2018, accessible at: https://www.disruptordaily.com/blockchain-use-cases-military-defense/.
- O'Brien, K. (2018). "China, Russia, USA in Race to Use blockchain for Military Operations" [online], Bitcoinist, published on September 22, 2018, available at https://bitcoinist.com/china-russia-usa-blockchain-military/ [last accessed on 11/03/2020].
- Rhodes, D. (2018). "Defense Industry Technology Could Improve Using Blockchain", *Coin Central*, published on June 15, 2018, accessible at: https://coincentral.com/defense-industry-technology/.
- Rothrie, S. (2018). "Blockchain Military Applications – the Future Tech of the Armed Forces", *Coin Central*, published on June 25, 2018, accessible at : https://coincentral.com/blockchain-military-applications-the-future-tech-of-the-armed-forces/.
- Sachdev, N. (2019). «US Army Looks to Blockchain to Secure Communications Data", *The Sociable,* published June 5, 2019, accessible at: https://sociable.co/technology/us-army-looks-to-blockchain-to-secure-communications-data/.
- Said Birch, S. (2015). "IBM's CEO on hackers: 'Cyber crime is the greatest threat to every company in the world'", *IBM Digital Nordic*, published on November 26, 2015, accessible at: https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/.
- Schmidt, J. (2020), "Driving trust: Distributed ledger for supply chain" [online], *Accenture*, published on January 20, 2020, available at: https://www.accenture.com/gb-en/insights/high-tech/blockchain-aerospace-defense [last accessed on 13/03/2020].
- Shen, M. (2018), "The Russian Military Is Building a blockchain Research Lab" [online], *Coindesk*, published on July 2, 2018, available at: https://www.coindesk.com/the-russian-military-is-building-a-blockchain-research-lab [last accessed on 12/03/2020].
- Vitu, JC. (2020). "Supply Chain et blockchain : un cyber-mariage parfait", *Economie Matin*, published on February 23, 2020, accessible at: http://www.economiematin.fr/news-blockchain-supply-chain-technologie-developpement-securite-vitu.
- Wood, M. (2019). "South Korea reveals blockchain plans for defense and arms procurement", *Ledger Insights*, published on August 2019, accessible at: https://www.ledgerinsights.com/south-korea-blockchain-defense-arms-procurement/.
- Young, L. and Desai, J. (2020), "blockchain's Promise for Defense Agency Supply Chains" [online], *Booz Allen*, available at: https://www.boozallen.com/s/insight/blog/blockchain-promise-for-defense-agency-supply-chains.html [last accessed on 13/03/2020].
- Guardtime Staff. (2019). "Defence Technology Institute of Thailand partners with Guardtime for Cybersecurity Research", *Guardtime*, published on January 31, 2019, accessible at: https://guardtime.com/blog/defence-technology-institute-of-thailand-partners-with-guardtime-for-cybersecurity-research

Official Documents

- NCI Agency (2016), "NCI Agency innovation challenge" [online], *NATO*, published on 25 April, 2016, available at: https://www.ncia.nato.int/NewsRoom/Pages/160425_Innovation.aspx [last accessed on 12/03/2020].
- European Commission (2017) "State of the Union 2017- Cybersecurity: Commission scales up EU's response to cyber-attacks" [online], published on 19 September 2017 available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193
- OECD (2018), *OECD blockchain Primer*, 2018, available at: https://www.oecd.org/finance/OECD-blockchain-Primer.pdf [last accessed on 12/03/2020].

- US DEPARTMENT OF HOMELAND SECURITY (2018), blockchain and Suitability for Government Applications, 2018, available at: https://www.dhs.gov/sites/default/files/publications/2018_AEP_blockchain_and_Suitability_for_Government_Applications.pdf [last accessed on 13/03/2020].

Books, Reports & Documentaries

- "Cryptocurrency" (2018), En Bref, *Netflix*, published in 2018.
- "KSI Blockchain" (2020), *e-Estonia*, accessed on March, 16 2020, at: https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/.
- ACT-IAC. (2018). "ACT-IAC White Paper: blockchain Paper for the US Federal Government". Published on April 23. Available at: https://www.actiac.org/system/files/blockchain%20Playbook%20w%20Integration%20Phase%20FINAL_0.pdf.
- Barberini, P. (2020), *Military Technology: Risks and Opportunities for the Atlantic Alliance*, Istituto Affari Internazionali/NATO Defence College, May 4, 2020.
- Deloitte (2016), *Israel: A Hotspot for blockchain Innovation*, Deloite Israel, Feb. 2016, available at: https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financial-services/israel_a_hotspot_for_blockchain_innovation_feb2016_1.1.pdf [last accessed on 11/03/2020].
- Deloitte (2019), *Deloitte's 2019 Global blockchain Survey*, Deloitte Insights, 2019.
- Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). *Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards*. Overview report The British Standards Institution (BSI), 34 p. Available at: https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf [last accessed on 19/03/2020]
- Dyèvre, A. and Mc Namara, S. (2018), "blockchain: Enjeux, usages et contraintes pour la Défense", *Les notes stratégiques*, CEIS, septembre 2018.
- European Defence Agency (2017), "blockchain Technology in Defence", European Defence Matters, issue 14, 2017, available at: https://eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence [last accessed on 13/03/2020].
- France Stratégie (2018), *Les enjeux des blockchains*, rapport, juin 2018, available at: https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf, [last accessed on 13/03/2020].
- Gottlieb, C. (2017), *blockchain in Aerospace and Defence*, Accenture report, 2017.
- Martinson, P. (2019) "Estonia – the Digital Republic Secured by Blockchain", *PwC*,, accessible at: : https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf.
- PwC Report. (2019). Estonia – The Digital Republic Secured by blockchain. PricewaterhouseCoopers. Available at: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf
- Schmidt, J. H., Gelle, M. and Wheless, J. (2018), "Launchpad to relevance. Aerospace and Defence Technology Vision 2018", *Accenture*, published on June 1, 2018, available at: https://www.accenture.com/us-en/insights/high-tech/launchpad-relevance AEROSPACE [last accessed on 13/03/2020].
- WFP (2020), "Building Blocks: Blockchain for Zero Hunger", available at: https://innovation.wfp.org/project/building-blocks [last accessed on 13/05/2020].
- Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. (2018) "blockchain Technology Overview", National Institute of Standards and Technology, US Department of Commerce.

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Chiefs of Staff in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and *ad hoc* coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

FINABEL
Quartier Reine Elisabeth
Rue d'Evere 1
B-1140 BRUSSELS

Tel: +32 (0)2 441 79 38 – GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at **www.finabel.org**

European Army Interoperability Centre

www.linkedin.com/in/finabelEAIC @FinabelEAIC @FinabelEAIC

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 441 79 38