ARTICLE

DOI 10.52781/cmm.a082

Cyberspace, Logistics and National Security Threats, Not Necessarily in that Order

Ciberespacio, Logística y Amenazas a la Seguridad Nacional, no necesariamente en ese orden

Marcelo Malagutti
Instituto Vegetius.
Brasília, DF, Brasil.
marcelo.malagutti@vegetius.org.br

Abstract: What is the relationship between cyber vulnerabilities, logistics and national security? Concerns about the potential exploitation of cyberspace vulnerabilities to cause logistical inefficiency in national security matters have lingered for nearly a quarter of a century. This article updates the landscape of this debate and extends the analysis to the reciprocal threats posed by these three areas. A descriptive methodology, based on case studies obtained from government sources, academic articles and news articles, is used to correlate cyberspace, logistics chains and national security threats. It is demonstrated that, in addition to common sense that the exploitation of existing cyber vulnerabilities at different levels of the increasing automation present in logistical systems presenting new threats that can disable military systems or civil infrastructures relevant to national security, there is a growing threat posed by the logistical complexity to cybernetic products and national security, as well as a 'weaponisation' of national security decisions of some countries that jeopardize supply chains, cybernetic or not, of other nations, with reflexes in the development of their defence capabilities.

Keywords: cyberspace; supply-chain management; strategic management.

Resumen: ¿Cuál es la relación entre las vulnerabilidades cibernéticas, la logística y la seguridad nacionalxxxx Preocupaciones sobre la posible explotación de las vulnerabilidades del ciberespacio para causar ineficiencia logística en asuntos de seguridad nacional han persistido durante casi un cuarto de siglo. Este artículo actualiza el panorama de este debate y amplía el análisis a las amenazas recíprocas que plantean estas tres áreas. Una metodología descriptiva – basada en estudio de casos hecho desde de fuentes gubernamentales, artículos académicos y artículos de noticias – se utiliza para correlacionar el ciberespacio, las cadenas de suministro y la seguridad nacional. Se muestra que, además del sentido común de que los ciberataques pueden explotar vulnerabilidades existentes en diferentes niveles de la creciente automatización presente en los sistemas logísticos, presentando nuevas amenazas que pueden inhabilitar sistemas militares o infraestructuras civiles relevantes para la seguridad nacional, existe una amenaza creciente planteada por la complejidad logística a los productos cibernéticos y a la seguridad nacional, así como una 'armamentización' (*weaponisation*) de las decisiones de seguridad nacional de algunos países que ponen en peligro las cadenas de suministro, cibernéticas o no, de otras naciones con repercusiones en el desarrollo de sus capacidades de defensa.

Palabras clave: ciberespacio; gestión de las cadenas de suministro; gestión estratégica.

Received: Oct. 22, 2021
Approved: Jul. 25, 2022

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 Introduction

It is already common sense that the exploitation of cyber vulnerabilities can disable or severely damage critical logistical systems and, thus, jeopardize national security. However, would this be the only causality order between these variables? This article argues that it is not. As it will show, empirical evidence confirms that supply chains can be used to compromise cyber capabilities and impact national security. Likewise, it is shown that national security decisions of a country affect logistics chains that create cyber vulnerabilities. Therefore, under certain conditions, the three factors may be causally related in any order.

To achieve this, it uses a descriptive research method of the *associations'* type (GERRING, 2012). The method is applied using the lenses of Strategic Studies thinking, looking for recurrent patterns of effective force (not necessarily the military one) to overcome opposing wills in conflict situations. This approach pervades the works of Clausewitz (1976), Liddell Hart (1930, 1931), Aron (2002), Beaufre (1965), Howard (1979), Freedman (1998, 2015), Gray (2008) and Stone (2007), to cite a few. The selection of cases and reference documents comprehended the last 10 years, with the notable exception of Eligible Receiver, used as a hallmark of the problem devised.

The article is structured as follows. After this introduction, a second section presents a brief introduction to logistics, while a third one shortly describes its encounter with cyberspace. A fourth section poses two classic examples of cyberattacks that compromised defence systems, showing the traditional order of causality relationship among the three variables analysed. A fifth section exemplifies the risks of logistical incapacitation of military forces in the theatre of operations, both from the point of view of supplies and that of communication and control, exemplifying the case of cyberattacks threatening logistics and national security. A sixth section presents threats posed by software and hardware manufacturing processes, with a supply chain comprising several contact points exploitable for implementing vulnerabilities. This situation points to logistics threatening cybersecurity and national security, with a subsection discussing governments' efforts to deal with them. A seventh section discusses the 'weaponisation' of the cyber supply chain, where national security decisions threaten the logistics of cyber products. Finally, brief considerations are made about the findings of this work.

2 A (Very) Brief Introduction to Logistics

A well-accepted definition of business logistics presents it as "the process of planning, implementing, and controlling the efficient and effective flow and storage of goods, services, and related information from the point of origin to the point of consumption for the purpose of conforming to customer requirements" (WOOD, 1998).

The study of Logistics as a science originated in the military. Vegetius, in the IV or V century, already dedicated significant parts of his work to the basics of military supplies provision (VEGETIUS, 1767). Despite this, the term itself derives from *Major General de Logis*, a military staff member whose duty "formerly was to lodge and camp the troops, to give direction to the marches of columns, and to locate them upon the ground" (JOMINI, 1862, p. 188). Over the years, that basic set of functions has been extended with the increased complexity of armies and battles. Interestingly, Clausewitz, often considered the most influenceable western war theorist, neither gave a definition of logistics nor used a specific term to describe it. This lead academics to argue that he considered it "all that is required so that the fighting force can be taken as a given" (PROENÇA JÚNIOR, DUARTE, p. 645).

Currently, in the military sciences, Logistics refers to "all the activities of armed-force units in roles supporting combat units, including transport, supply, signal communication, medical aid, and the like" (LEIGHTON, 2022). The difficulty of finding a specific term that can, without prejudice, encompass and define precisely this elaborate list of activities still remains nowadays (LEIGHTON, 2022). The importance of logistics for the military is, indeed, expressed by the quote "amateurs talk tactics, but professionals talk logistics", "attributed to everyone from Napoleon Bonaparte to Omar Bradley" (EPSHTEIN; FAINT, 2019).

Supply chains are the flows of goods and information within and among organisations, "linked by a range of tangible and intangible facilitators, including relationships, processes, activities, and integrated information systems" (PECK, 2012, p. 196). They are "the mechanism at the heart of globalisation of the past few decades by which raw materials, parts and components are exchanged across multiple national boundaries before being incorporated into finished goods" (SUPPLY..., 2019).

The acquisition, storage, and distribution of hundreds of thousands of items of ammunition, armaments, vehicles (with their corresponding spare parts and maintenance services), fuel, uniforms, accommodation, food, health and hygiene, with complex supply chains, which must operate in difficult terrain, with restricted means of transport and in combat conditions, is a task of enormous complexity.

Fuel and armaments shall be stored in a combat zone with enough ammunition for defending it. Otherwise, the enemy could take those stocks of fuel and armaments, with a double negative impact: missing them and having them used against their original owners. Therefore, it is essential to have only the necessary and sufficient of each supply item in each area of operations. The same principles apply to civilian logistics: corporations seek to eliminate unnecessary stocks with the same effort with which they try to avoid the unavailability of items that could compromise their operations.

Despite operating in different scenarios, military and civilian logistics chains, thus, pursue the same primary objectives. Focus is no longer *mass-oriented*, but *velocity-oriented*, with only necessary and sufficient stocks, reliable distribution, adequate costs, reliable supply chains and *just-in-time* or *on-demand* delivery (KRESS, 2002).

3 Where Logistics and Cyber Meet

Effectiveness, the resulting combination of efficiency (doing things right) with efficacy (doing what needs to be done), is an imperative for logistics. As such, automation has been historically attached to supply chain management.

Modern logistics demands dynamic information about the entire supply chain, named 'In-Transit View' (KRESS, 2002). Such controls are strongly supported by computerised systems, whatever the form of contracting, cost control, inventory or distribution adopted. Data generated at scattered points, whether from claimants, suppliers or transporters, are collected and processed in an integrated manner in real-time. The user informs his position and need; the system checks the availability of suppliers and informs the price and estimated time of arrival (ETA) to the user, who may or may not confirm the order. If acceptance is established, the user can follow the item's movement towards him and the adjusted ETA in real-time.

Similarly, computerised systems allow to scale demand, determine the location and size of inventories, demand suppliers, sometimes even without human interaction, to control and monitor the distribution of items, and also to determine the change of plans operational, providing 'total asset visibility' (KRESS, 2002).

Autonomous vehicles, as well as artificial intelligence, "may fundamentally alter how supply chains operate and use their integrated data, systems and assets"; these new levels of automation shall increase efficiency and reduce operational costs (TURNBULL, 2018, p. 45). As a fundamental part of what is now called Industry 4.0, it is expected that Additive Manufacturing (3D printing) might make possible the local production of items and spare parts on demand, thus simplifying transportation and storage needs and associated risks. In 2015 the U.S. Army Engineer Research and Development Center Construction Engineering Research Laboratory established the Automated Construction of Expeditionary Structures (ACES). It aims to develop reliable user-friendly 3D printing technology capable of generating custom-designed military expeditionary structures on demand, in the field, using locally available materials (JAGODA et al., 2020, p. 2). In January 2021, the U.S. DoD released its Department of Defense Additive Manufacturing Strategy to align 3D printing with the DoD mission (UNITED STATES, 2021a, p. 4). The U.S. military already can "print" replacement parts for submarines, Humvees and even B-52 strategic bombers, and ordered a shipping container-sized portable 3D manufacturing unit that could be deployed on land and sea (BURTON; MCBIRNEY, 2022; SCHWAAR, 2022).

Nonetheless, despite how vital the pros of increased automation are, they also carry relevant cons. With the push for automation, logistics systems will become increasingly connected and targetable (TURNBULL, 2018). Not surprisingly, the U.S. DoD report issued in 2022, in attention to the Executive Order on America's Supply Chains from 2021, makes 88 references to "cyber" terms, more than a third of the 251 references to "supply chain" (BIDEN JR, 2022; UNITED STATES, 2022a).

Technological advances raise the spectre of an arms race in supply-chain security, with private and state-sponsored hackers having the upper hand over corporations and governments (SUPPLY..., 2019). Moreover, supply chains are already one of the "three main vectors of cyberattack" (along with networks and human insiders) (NYE JR, 2017, p. 50). Hence, much effort is yet to be made to secure supply chains from attacks through computing devices (LEE; MOLTKE, 2019).

4 Cyberthreats to National Security Logistics Systems

This section presents the classic case of cyber threats risking logistics relevant to National Security.

Almost a quarter of a century ago, in June 1997, the U.S. Joint Chiefs of Staff carried out an exercise named *Eligible Receiver* to test American cyber defences. The proposed scenario was that of a crisis that would force Washington to quickly send troops and aircraft to South Korea. Thirty-five experts from National Security Agency (NSA) made up the 'red team', simulating hackers in the service of North Korea with the mission of subverting the American operation, using only publicly available equipment and information. In just two weeks, using only commercial computers and hacking programs downloaded from the Internet, this red team could "simultaneously break into the power grids of nine American cities and crack their 911 emergency systems" (ADAMS, 2001, p. 101).

"Having ensured civilian chaos and distracted Washington", hackers attacked the Pentagon's computer networks, becoming able to "roam freely across the networks, sowing destruction and distrust wherever they went" (ADAMS, 2001, p. 101). For example, directing supplies to wrong destinations, potentially crippling state-of-the-art combat aircraft due to a lack of fuel, spare parts and weapons (ADAMS, 2001).

Similarly, the exploitation of cyber vulnerabilities in military logistics could be behind the disabling of radar and computerised anti-aircraft batteries, as the Israelis arguably have done in Operation Orchard before embarking on an airstrike against Syria's alleged nuclear facilities in Deir Ez-Zor (LIFF, 2012).

Currently, the U.S. Defense Science Board (DSB) considers the impacts of a cyberattack against supply chains to be potentially spectacular. Whenever the U.S. is in conflict, it must wait for cyberattacks intending to corrupt its supply chains, make its missiles and bombs not work, or even use them against the American troops themselves. Supplies, including food, water, ammunition, and fuel, could not reach where or when needed. Military commanders would quickly lose confidence in information and the ability to control their systems and forces. Once lost, trust is arduous to recover (UNITED STATES, 2013b).

In 2013/14, the U.S. Senate Committee on Armed Services investigated cyberattacks involving the U.S. Department of Defense (DoD) Transport Command (TRANSCOM) and eleven of its suppliers. The resulting report notes that the committee focused on TRANSCOM due to its central role in 'mobilization, deployment, and sustainment operations and the critical capabilities that TRANSCOM contractors provide to meet military requirements in contingency operations' (BRYAN et al., 2014). The report states that private airlines provide more than ninety per cent of the passenger handling capacity and more than a third of the DoD's gross cargo handling capacity, while 95% of its dry cargo is transported by merchant ships. In addition, more than 90% of DoD deployment and distribution transactions occur in non-classified networks, many of which belong to private companies, according to an estimate by the TRANSCOM commander (BRYAN et al., 2014).

The TRANSCOM investigation identified 50 cyberattacks or intrusions carried out between June 1, 2012, and May 30, 2013. Also, at least 20 successful intrusions into contractor networks were classified as Advanced Persistent Threats (APT). The term is "used to distinguish sophisticated cyber threats that are frequently associated with foreign governments"; of these, the command was informed of only two, "a worrying finding, given the potential impact of cyberintrusions on defense information and operations" (BRYAN et al., 2014, p. i).

Among the reasons why TRANSCOM was unaware of the attacks, it was found that there were gaps in the contractual communication requirements, in addition to the lack of a common understanding between the contractor and its contractors as to the scope of what should be reported regarding cyberattacks. Besides, the Federal Bureau of Investigations (FBI) and DoD were often unaware that companies identified as victims of cyberattacks were suppliers to that command (BRYAN et al., 2014).

The U.S. Defense Logistics Agency (DLA) Strategic Planning 2015-2022 established that cybersecurity constitutes a significant operational risk that imposes severe challenges on DLA supply chains at all times. Thus, it is necessary to create an environment that stimulates reporting and combating cyber threats and that the same attention should be extended to its supplier base, where DLA must be 'astute' in relationship management to ensure that private sector partners protect supplies and the integrity of data to effectively provide support to combatants (UNITED STATES, 2015). The intended cunning may be reflected in using PBL to' stimulate' suppliers.

The U.S. Senate investigation found that all APTs identified in TRANSCOM and its suppliers were assigned to China. It also indicated that Chinese military analysts identified logistics and mobilisation as potential U.S. vulnerabilities, 'given the requirements for precision in coordination, transportation, communications, and logistics networks' and that Chinese military doctrine 'advocate[s] targeting adversary command and control and logistics networks to impact their ability to operate during the early stages of conflict'. Moreover, the investigation found that American experts in Chinese military planning raised the possibility of China using cyber capabilities to prevent the deployment of U.S. forces in the event of a contingency (BRYAN et al., 2014). Thus, the Chinese could seek to obtain, in an eventual conflict with the USA, the same advantages obtained by the NSA red team in Eligible Receiver, 25 years ago.

Possibly the most relevant effect of Eligible Receiver was the fact that hackers were also able to paralyze the human Command and Control (C2) system with a high level of distrust stemming from a commanding General's false orders, forging "bogus news reports on the crisis and instructions from the civilian command authorities" (ADAMS, 2001, p. 101).

> "As a result, nobody in the chain of command, from the president on down, could believe anything. This group of hackers using publicly available resources was able to prevent the United States from waging war effectively" (ADAMS, 2001, p. 101).

C2 is also a military logistics function. Although non-intrinsically a cyber military capability as many others, it became so dependent on cyberspace that an opponent might be tempted to seek a first disabling cyberattack on them (MORGAN, 2010). This process of cyber-C2-degradation, aimed at destroying (or at least largely degrading) the opponent's internal cohesion, could potentially incapacitate the military forces of the targeted foe and increase the effectiveness of a subsequent kinetic attack against them.

Moreover, modern weaponry has been increasingly dependent on integrated circuits, and today electronics contain programmable code of increasing complexity. At the same time, DoD has become a much less influential buyer in a vast and globalized supplier base. Because of this, ensuring that electronic defence components are free of vulnerabilities is a Herculean task (UNITED STATES, 2017).

Since the configuration settings of these devices remain unchanged for long periods, compromised components can create persistent vulnerabilities, and exploiting these vulnerabilities in components or their embedded software can cause modern weaponry to fail. Such explorations are particularly harmful because it is difficult to differentiate them from electrical or mechanical failures.

Besides, a cyber-attack itself does not need to be lethal. If it degrades the effectiveness of a military force or reduces the functionality of precision weapons and targeting systems or the availability of fuel and medical supplies, the result will be deadly for the force-dependent on compromised resources (TURNBULL, 2018).

Still, in the realm of National Security, besides the cyber threats to military logistics and C2, there is also the often-mentioned cyber threat to civilian critical-infrastructure. Until recently, the most famous cases had been those involving the Ukraine power supply in 2015, named Industroyer, and 2016, named CrashOverride, arguably launched by Russian hackers (AUCHARD; FINKLE, 2016; ZETTER, 2016). However, in May 2021, a ransomware attack attributed to a Russian cybercriminal group named DarkSide, hit the Colonial Pipeline, leaving vast parts of the U.S. with restricted supplies of petrol derivates (SANGER; PERLROTH, 2021).

5 Logistical Threats to Cyber Products

This section discusses the case where logistics threaten cyber products and National Security. It is common sense that a screw, fuse or chemical component tampered with in a long and difficult to control supply chain can affect the performance of, or create physical vulnerabilities in, any military equipment. A less perceptible understanding, however, is that similarly, components tampered with in the extended supply chain of hardware or software products can affect the performance of or create vulnerabilities in them and the systems that use them. To better capture this concept, it is necessary to understand the cyber products' supply chain, which the U.S. National Institute of Standards and Technology (NIST) calls the Cyber Supply Chain (NIST; FIREEYE, 2015).

As early as 2001, American intelligence officials believed 'that certain equipment and software imported from Russia, China, Israel, India and France' were infected with 'devices' capable of 'reading data and destroying systems', although this suspicion was difficult to prove (ADAMS, 2001). Recently, counterfeit hardware was identified in systems acquired by DoD (LYNN III, 2010). As a result, a report by the U.S. House Permanent Intelligence Commission in 2012 restricted the purchase of equipment from Chinese companies Huawei and ZTE (ROGERS; RUPPERSBERGER, 2012).

Current digital systems are highly complex, built by overlapping software and hardware components integrated into different levels and provided by various suppliers from diverse parts of the world. The materiality of hardware makes it easily perceivable, and humans are more prone to understand and accept it as risky or unsafe. Nevertheless, software is what 'animates' hardware.

At the very basic software level, electronic devices are usually controlled by *firmware*, software recorded on their components. It determines how the equipment operates. A famous example is the Basic Input Output System (BIOS) of processors, but it also exists on network and video circuit boards, scanners, or printers. Increasingly, hardware offers the possibility of updating its firmware, thus changing the device's operational behaviour without needing to replace it. Malware can exploit firmware vulnerabilities, for example, by inserting a kill switch that could deactivate the hardware under enemies' orders. Possibly worse, malware can make devices behave erratically.

The firmware uses another software layer, the *driver*, to communicate with *Operating Systems* (OS) like Android, iOS, Windows or Linux. The same hardware-firmware pair (a printer, for instance) has different drivers to communicate with different OS. A tampered driver can modify how a device operates, deceiving the OS. This was the principle behind Stuxnet, where the Programming Logic Controllers (PLCs) connecting the Iranian uranium enrichment centrifuges to their Supervisory Control And Data Acquisition (SCADA) system were replaced by tweaked ones. Hence, while the control system indicated the centrifuges were regularly operating, they were actually spinning out of pace and thus being physically damaged (ZETTER, 2015a).

At a higher level, it is possible to contaminate the OS itself. In the Snowden case, it was revealed that Cisco, the world's largest manufacturer of network assets, had its routers and servers' OS (Cisco IOS) manipulated by the NSA (GREENWALD, 2014). In December 2015, Juniper Networks, the second-largest manufacturer of network assets, announced the discovery of a secret backdoor in JunOS, the OS of its firewalls. It was found that it had been inserted into the code before 2011 (ZETTER, 2015b). It did not become clear who would have implanted that backdoor.

In August 2016, Cisco, again, announced the discovery of a 0-day (factory) vulnerability in Cisco IOS, implanted 13 years before, that could be exploited to ensure full access to networks using their equipment. It was found when analysing program-code allegedly belonging to the Equation Group (hackers linked to the NSA) that was 'leaked' on the Internet by hackers group Shadow Brokers (GOODIN, 2016). Hence, the NSA could have exploited this vulnerability to breach computer networks of U.S. interest. Cisco found at least eight other similar backdoors in its OS in 2017 and 2018 (CIMPANU, 2018; CISCO, 2017).

The following software level is called *middleware*, the "software that lies between an operating system and the applications running on it", "[e]ssentially functioning as hidden translation layer", and enabling communication and data management for applications (MICROSOFT, 2022). This category includes database and web servers, among others. Applications (Apps) connect to them thru software libraries called Application Programming Interfaces (APIs) or Software Development Kits (SDKs). These APIs, which are often developed by third-party suppliers in different parts of the world, can be tweaked in the integration process.

Almost at the top software layer is the Commercial-Off-The-Shelf (COTS) software, like office automation platforms, e-mail systems, pdf generators and readers, and hundreds of others. Weaponised Adobe Portable Document Files (PDFs) and Microsoft Office documents have been compromising systems for a while (HUTCHINS; AMIN; CLOPPERT, 2010).

Finally, the top software layer is that of specialised applications, which run the 'core businesses' of organisations, such as logistics systems. The complexity of modern applications has turned software development into assembly, in a context of collaborative development, with very specialized components (APIs) acquired from third parties, thus creating very long supply chains (SHERMAN, 2019).

Much of these components are *black boxes*, with their source code invisible, although Open-Source Software (OSS) is gaining space in the software industry and acceptance within the military (UNITED STATES, 2021b). The software supply chain has become a complex web of components within an organisation's trusted downloaded components of code used to build applications (BLESSMAN, 2019). Furthermore, software is 'extremely malleable under pressure from the right combination of finger strokes, which can bring both strategic advantages and weaknesses when embedded in the world through dependence on connected technology' (WOODS; BOCHMAN, 2018).

Overall, this complexity makes it crucial to keep these multiple components up-to-date, and ongoing software patch management is necessary. The management of software patching is complicated by the fragility of production environments where a multitude of applications and supporting packages must interact without causing conflicts or catastrophic failure (TURNBULL, 2018).

Moreover, a tweaked version of software of a Ukrainian accounting firm containing a destructive payload, named NotPetya, paralyzed networks globally, costing FedEx and Maersk, two logistic giants, more than $300 million each (UNITED STATES, 2018). Software update mechanisms (delivery systems, indeed!) were abused to gain access to grid control systems (WOODS; BOCHMAN, 2018).

In another famous case, in 2017, circa 2.2 million customers were infected with a backdoor when hackers, targeting companies like Samsung, Sony, Asus, Intel, VMWare, O2 and Fujitsu, hijacked the automated update system of CCleaner, an anti-virus and security software (CORERA, 2018; UNITED STATES, 2018).

Recently, investigations revealed that SolarWinds, a U.S. company that produces an IT network management software named Orion, had been infected as early as October 2019. The compromise of that supply chain allowed the use of Orion's routine software security update to install malicious software in SolarWinds customers' networks. This compromise ensured the hackers' access to at least nine U.S. federal agencies, including the Department of Treasury and the Department of Justice, and to "major digital-technology outfits such as Cisco, Intel, Nvidia and Microsoft, as well as cyber-security companies like FireEye" (WILLETT, 2021, p. 8).

The software supply chain complexity challenges most corporate security programmes, since tampered components become hard to detect, and "organizations simply trust that their vendors are providing secure software, offering threat actors a workaround for defeating an organization's security procedures" (BLESSMAN, 2019, p. 10).

Vulnerabilities in the supply chain can be inserted or discovered over the entire life cycle of a software product, giving particular concern to the fact that most systems are developed, acquired, and distributed without formal protection plans (UNITED STATES, 2017).

Dealing with the Cyber Supply Chain

The 2011 DoD Strategy for Operating in Cyberspace posed supply chain vulnerabilities and threats to DoD's operational ability as one of the 'central aspects of the cyber threat' (UNITED STATES, 2011). It also states:

> Software and hardware are at risk of malicious tampering even before they are integrated into an operational system. The majority of information technology products used in the United States are manufactured and assembled overseas. The reliance of DoD on foreign manufacturing and development creates challenges in managing risk at points of design, manufacture, service, distribution, and disposal (UNITED STATES, 2011, p. 3).

Intuitively, one might feel tempted to propose that the government should approve foreign hardware and software before they enter the market. In practice, however, this would not be viable. The number of lines of source code (SLOC) for commercial software products has grown to approximately fifty million, and the U.S. government believes this growth will continue for the next decades (UNITED STATES, 2013b). On the hardware side, complex integrated circuits today have more than two million transistors. It is, therefore, impossible to thoroughly test the flaws and vulnerabilities of such software or hardware products. Trying to check them fully would take years.

These complex products often enter the market with bugs. For example, in 1994, just after the brand new Pentium processors entered the market, a bug in its floating-point number division, making it considerable imprecise, was unveiled (HALFHILL, 1995). Again, in 2020, a new flaw was discovered in all of the company's processors produced in the last five years that could be explored to gain access to the system security (BLUMENTHAL, 2020).

In 2014, NIST published its Framework for Improving Critical Infrastructure Cybersecurity in a partnership between the U.S. government and the private sector, bearing in mind that 'similar to financial and reputational risk, cybersecurity risk affects a company's bottom line' (NIST, 2014). The central principle is that cybersecurity in the supply chain is not just about information and communication technology (ICT) but involves suppliers, resellers, management, supply chain continuity and reliability, transport security and other security activities.

Based on its framework, NIST started to research not only ICT companies but also companies that use ICT products widely in their processes. Among the participating companies are Boeing, Cisco, Deere, Dupont, Fire Eye, Fujitsu, Intel, Juniper, Northrop Grumman, P&G and utilities (or infrastructure) companies. The objective was to detect how companies deal with issues like the ones below (NIST, 2014):

- Third-party suppliers with physical or virtual access to information systems, source codes of programs or equipment (from cleaning to software engineering);

- Inadequate information security practices by its suppliers;

- Compromised hardware or software products purchased from suppliers;

- Software security vulnerabilities in supply chain management or supplier systems;

- Counterfeit hardware or embedded malware;

- Data storage or data aggregation by third parties;

- Repeatability and traceability of the software or hardware design and development process;

- Supplier's capabilities to address vulnerabilities, including 0-day.

Hence, there is a growing concern of the U.S. government regarding the guarantee of Cyber Supply Chain Risk Management (C-SCRM) with its suppliers, and these with theirs, recursively (NIST; FIREEYE, 2015).

When a government purchases products or services with inadequate *factory* or *built-in* security, risks persist throughout the life cycle of the purchased item. This long-lasting effect is part of what makes changing procurement processes so important to achieve cybersecurity and resilience. Buying products and services with the appropriate built-in 'factory' security may have higher upfront costs. Still, it reduces the total cost of ownership (TCO) due to risk mitigation and the reduced need to correct vulnerabilities in products distributed or deployed in the field (UNITED STATES, 2013a).

In typically long DoD procurement processes, about 70% of electronics in weapon systems are obsolete or out of production before these products are deployed (UNITED STATES, 2017). This causes new components to be inserted during the production process, which makes validating the integrity of these components even more difficult.

As a result, malware can be deployed to computer systems (hardware + software) as they are developed or built and potentially used to create remotely operated kill-switches and backdoors, allowing intruders to manipulate the systems running on it in conflict situations. To contain this risk, private software and hardware companies in the United States have become governmental partners in creating security mechanisms. For example, Microsoft and other computer companies develop sophisticated strategies to detect malicious code (such as the back doors of Juniper Networks and Cisco) and prevent its deployment in their global supply chains (LYNN, 2010). Despite, in March 2021, a failure in Microsoft's e-mail server product Exchange was used by Chinese hackers to gain access to users' data and e-mails, affecting 'up to 30,000 public and private entities, mainly small businesses and local governments' (WILLETT, 2021).

6 National Security Weaponisation of the Cyber Supply Chain

At last, this section describes how National Security decisions regarding export and import restrictions weaponize cyber supply chains, posing threats to the cyber logistics chain of other countries. This exemplifies the third case studied, where National Security decisions affect cyberspace and logistics chains in foreign countries.

Since 2015 the U.S. government has prevented Intel from reselling its most modern processors to China, allegedly because they would be used for nuclear tests (CLARK, 2015). In 2018, the country regained the top two positions on the supercomputer list, previously occupied by China (TOP500.ORG, 2020). The difference among the processors is reflected in the numbers shown. While U.S. Sierra, in the first place, reaches 200 PFLOPS with 2.4 million cores and consumes 10 MW of energy power, the Chinese TaihuLight, third in the list, using Chinese processors, reaches 125 PFLOPS with 10.6 million cores and consumes 15 MW (TOP500.ORG, 2020).

The preferred Chinese solution, typical of any developing country, is replacing foreign solutions with indigenous ones, a solution that requires a strong innovation capability and, counterintuitively, global connections (LEWIS, 2018). China uses "national champions, protects them in the domestic market, and helps them compete" globally (LEWIS, 2018, p. 5-6). "[I]f China had not blocked Google, there would be no Baidu" (LEWIS, 2018, p. 5-6). However, "[t]his promotion of national champions by any means is the source for much of the current trade tensions, and Western governments are slowly developing responses that will constrain China's growth unless its policies change" (LEWIS, 2018, p. 5-6)

More than 25 centuries ago, Sun Tzu wrote:

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle (TZU, 2009, p. 13).

Having intelligence information is part of statecraft common sense. Furthermore, intelligence agencies are always looking for opportunities of gathering sensitive information thru ICT networks and devices, even in peacetime, and related to traditional partners and allies. Not even equipment provided by companies from traditionally neutral countries can be considered unsuspected and unreachable by their tentacles. For example, Swiss company Crypto AG, a manufacturer of cryptographers used in more than 120 countries, belonged, between 1970 and 2018, to a highly secretive partnership between the CIA and the German intelligence service BND. Crypto AG equipment was sabotaged so that those agencies could access the information those devices encrypted (MILLER, 2020). In another famous case, Snowden left clear that the NSA was spying on dozens of U.S. allies, including Germany, Brazil, Japan and Mexico (GREENWALD, 2014).

Now, the U.S. government accuses Huawei, the world leader in 5G telephony, of having obscure connections with Chinese intelligence. Moreover, the U.S. argues that it prefers the use of equipment from Swedish Ericsson or Finnish Nokia, even if more expensive, and personalities of the U.S. government have even suggested the acquisition of shares for controlling these companies (KHARPAL, 2020).

The United States is also pressuring its allies to veto the use of Chinese 5G technology. In May 2020, the United Kingdom announced a ban on the company from acting. The German Deutsche Telekom (32% state-owned) answered that excluding Huawei from their 5G networks would be 'Armageddon', and although not restricting its participation, recently announced that Ericsson was chosen (ALLEVEN, 2020; ERICSSON, 2020; PETZINGER, 2020). Under enormous pressure from the U.S. regarding the participation of Huawei in Brazilian networks, with the U.S. ambassador threatening 'consequences', the Brazilian military reportedly told their government that "the same eventual exposure that

Brazil may suffer from Chinese technology with Huawei will also occur with any other company" (AMADO et al., 2020; ROSA; ANTUNES, 2020). Indeed, a very pragmatic position, considering the Crypto AG, Cisco and Juniper cases, among others.

On the Chinese side, in 2017, a new cybersecurity law restricted the sale of foreign information and communication technology. In addition, China demanded that foreign companies submit these products to government-administered National Security reviews, and that firms operating in China store their data in China, requiring official approval before being transferred to other countries (UNITED STATES, 2018). As it is clear that security reviews shall be long and imperfect, this seems to be a way of creating barriers for foreign technology, a counterstrike due to Huawei's western restrictions.

Excluded from the U.S. market in 2019, Huawei responded by banning the use of North American components. The Chinese giant began to work to replace these components with Chinese versions (STRUMPF, 2020). However, even that strategy was threatened when the U.S. Department of Commerce stepped up in May 2020 and banned component manufacturers using U.S. technology worldwide from selling products to Huawei (UNITED STATES, 2020). This new difficulty can even take the company out of its dominant position in the 5G race and jeopardize the maintenance of telephone networks of other generations provided by the company and already in use in several countries (STRUMPF, 2020). In addition, the U.S. is now considering blocking the supply of U.S. technology to five Chinese video surveillance companies (SHIDONG, 2019).

Restrictions on use do not only refer to hardware, but also software. The U.S. government's ban on Huawei prevents Google from licensing the use of Android OS on company phones (MOON, 2019). Although Android's core is open source, so it can continue to be used by the Chinese company, several associated services are provided by Google and would no longer be available, limiting the usefulness of Huawei's smartphones (MOON, 2019).

Amidst the U.S. embargo on supplying technology to China, Beijing has ordered all government offices and public institutions to remove foreign equipment and software by 2022 (YANG; LIU, 2019). The move is part of a campaign to reduce Chinese dependence on foreign technologies, is likely to decouple supply chains between the U.S. and China, and could mean a significant blow to U.S. companies (YANG; LIU, 2019). The new sanctions imposed added urgency to the project. Unlike previous efforts for self-sufficiency in technology, the goal is that companies and the government will soon be free from threats (YANG; LIU, 2019).

Nonetheless, replacing U.S. hardware and software with Chinese equivalents also poses problems. China's Lenovo uses processors made by Intel and hard drives made by South Korean Samsung (YANG; LIU, 2019). China lags behind the U.S. in some of the most advanced technologies, including chip design and manufacturing. Intel and Qualcomm manufacture the main components of some of the country's largest technology companies.

The OS most used on devices produced in China is Google Android, on smartphones and tablets, or Microsoft Windows, on computers (SHIDONG, 2019).

In 2019, the U.S. elevated the tone with the Executive Order on Securing the Information and Communications Technology and Services Supply Chain, which states:

> Unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States (TRUMP, 2019, n. p.).

Then, in 2020, the U.S.-China clash gained a new chapter, involving the TikTok App, used for posting short videos, controlled by Chinese-owned company ByteDance, allegedly posing threats to National Security. It is not yet clear what would be those threats, but it is important to observe that National Security relevant information can be obtained from unsuspected sources. In 2018, data from a harmless fitness tracking app called Strava revealed the location of U.S. Army secret bases worldwide. The company released maps that would identify 'popular running routes in major cities, or spot individuals in more remote areas who have unusual exercise patterns'. Nevertheless, "military analysts noticed that the map is also detailed enough that it potentially gives away extremely sensitive information about a subset of Strava users: military personnel on active service" (HERN, 2020).

Whatever the reason, in the Tik Tok case, the U.S. government intended to force its local operation to be sold to an American-owned company. The legal support is provided by the Committee on Foreign Investment in the United States (CFIUS) under the Defense Production Act of 1950 (UNITED STATES, [2022b]). CFIUS can block the acquisition of American companies by foreign investors. In 2018, TikTok, then named Music.ly, also a Chinese company, was bought by ByteDnce. But Music.ly, despite being Chinese, under CFIUS regulations, is considered 'U.S. business' as an entity that engages in interstate commerce in the United States. Thus, CFIUS can force the U.S. operation to an American-owned company since ByteDance has not asked for CFIUS approval at the time of the acquisition (CHESNEY, 2020).

7 Conclusion

This article sought to demonstrate how Cyberspace, Logistics, and National Security pose severe threats one to the other. Not necessarily in the usual perceivable order of causality, but in any chosen order. A prolific set of dozens of cases, involving majorly cyber powers such as the United States and China, as well as the United Kingdom, Germany and other nations' governments and private companies, has provided robust empirical evidence to sustain this argument.

First, it has shown how the demand for better logistics leads to increasing automation, thus for more computerised logistics support. This crescent automation, along with the use of increased digital communications, autonomous vehicles, artificial intelligence and additive manufacturing (3D printing), among other new technologies, poses growing risks of exploiting cyber vulnerabilities and allowing for the logistical incapacitation of military forces and societies. Hence they present many opportunities for compromising National Security. Since 2018, there has been an increased pace of measures taken (or initiated) by the governments of cyber powers aimed at reducing this risk. Nevertheless, as argued by this piece, this was the classic and more common-sense perception.

Second, much less evident than the first one, the article showed how increasingly complex logistics pose risks to the reliability and performance of hardware and software products. As shown, in a similar way that a tweaked electro-mechanical component infiltrated anywhere in the extensive supply chain of a military equipment, maliciously altered software or hardware components can compromise its reliability or performance. Hence, it also affects National Security. To achieve this, it presented the concept of cyber supply chains, and how its complexity transcends national borders, demanding much research and investments to create and maintain controls that increase the security of these products, while fluid enough not to make their development too rigid and time demanding. A concrete fact that complicates this control is that hardware and software production chain is highly complex, with many points of contact distributed in different parts of the world. Exemplifying, computers made in Brazil can simultaneously have circuits and chips designed in the USA, Germany and Japan, and produced in China, Taiwan, Singapore, Vietnam and India, whose firmware was produced in many other countries. Likewise, the large and complex modern software systems are also built in development centres spread over several countries by technicians from other countries.

Third, it was also demonstrated how National Security based decisions, such as the restriction of exporting (or importing) IT components to or from foreign countries, can compromise either hardware and software supply chains (logistics) and the pace of the development of cyberspace. Not only in those nations that are their primary targets, but also in those who implement these measures. As explained, substituting foreign-provided components with indigenous (or 'neutral' third party) ones, if not a Herculean task as the control of the cyber supply chain, is also an expensive and time-demanding effort.

Overall, the article shows that the perception has evolved from a static threat, closed within the perimeter of the nation, government or defence production, to a dynamic danger present throughout the entire supply chain, notably private suppliers.

The bad news is that securing all three areas is a very complex task. Moreover, its feasibility still requires much research, particularly concerning high-tech assets in the Defence Industrial Base, the companies that supply governments with products and services related to National Security.

The good news is that huge efforts have already been made on the subject at the international level, with abundant material available, which allows us to save time and resources to implement several practices adopted by the world-class industry. More importantly, there is an increasing perception that the subject needs to be treated accordingly to its relevance.

For now, the only certainty is that global supply chains related to cyberspace and National Security will be under much more scrutiny than they are nowadays. Furthermore, a considerably larger nationalistic approach can be expected, possibly (or probably) profoundly changing what has been considered the core of recent globalisation tendency.

Acknowledgements

The author thanks the peer-reviewers who contributed to this work's improvement.

References

ADAMS, James. Virtual defense. **Foreign Affairs**, [New York], v. 80, n. 3, p. 98, May/June 2001.

ALLEVEN, Monica. Deutsche Telekom selects Ericsson for 5G RAN in Germany. **FierceWireless**, [*s. l.*], July 22, 2020. Available at: https://www.fiercewireless.com/operators/deutsche-telekom-selects-ericsson-for-5g-ran-germany. Access on: July 28, 2022.

AMADO, Guilherme *et al*. O recado das Forças Armadas ao Ministério da Defesa sobre o 5G. *Época*, 7 ago. 2020. Available at: https://epoca.globo.com/guilherme-amado/o-recado-das-forcas-armadas-ao-ministerio-da-defesa-sobre-5g-24571588. Access on: July 28, 2022.

ARON, Raymond. **Paz e guerra entre as nações**. São Paulo: Imprensa Oficial do Estado, 2002.

AUCHARD, Eric; FINKLE, Jim. Ukraine utility cyber attack wider than reported. **Reuters**, [Eagan], Jan. 3, 2016. Available at: http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UI23S20160104. Access on: July 28, 2022.

BEAUFRE, André. **Introduction to strategy**. London: Faber and Faber Limited, 1965.

BIDEN JR, Joseph R. Executive Order on America's Supply Chains. *In*: THE WHITE HOUSE. Washington, DC: The White House, Feb. 24, 2022. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/. Access on: Aug. 1, 2022.

BLESSMAN, Danika. Protecting your software supply chain. **Risk Management**, [*s. l.*], n. 1, p. 10-11, 2019.

BLUMENTHAL, Eli. 'Unfixable' hole in Intel ROM exposes all but latest chips to attack, researchers say. **CNet**, [*s. l.*], Mar. 6, 2020. Available at: https://www.cnet.com/news/unfixable-hole-in-intel-rom-exposes-all-but-latest-chips-to-attack/. Access on: Aug. 3, 2022.

BRYAN, Joseph M. *et al*. **Inquiry into cyber intrusions affecting U.S. Transportation Command contractors**. Washington: U.S. Senate, 2014. Available at: https://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf. Access on: Aug. 3, 2022.

BURTON, Phillip; MCBIRNEY, Samantha. Military yet to fully leverage additive manufacturing. **National Defense**, Arlington, VA, Feb. 16, 2022. Available at: https://www.nationaldefensemagazine.org/articles/2022/2/16/military-yet-to-fully-leverage-additive-manufacturing. Access on: Aug. 3, 2022.

CHESNEY, Robert. TikTok and the law: a primer (in case you need to explain things to your teenager). **Lawfare**, [*s. l.*], Aug. 2, 2020. Available at: https://www.lawfareblog.com/tiktok-and-law-primer-case-you-need-explain-things-your-teenager. Access on: Aug. 3, 2022.

CIMPANU, Catalin. Cisco removed its seventh backdoor account this year, and that's a good thing. **ZDNet**, [*s. l.*], Nov. 7, 2018. Available at: https://www.zdnet.com/article/cisco-removed-its-seventh-backdoor-account-this-year-and-thats-a-good-thing/. Access on: Aug. 3, 2022.

CISCO. **Cisco prime home authentication bypass vulnerability**. San Jose, CA: Cisco, Feb. 2017. Available at: https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20170201-prime-home.html. Access on: Aug. 3, 2022.

CLARK, Don. U.S. Agencies block technology exports for supercomputer in China. **The Wall Street Journal**, New York, Apr. 9, 2015. Available at: https://www.wsj.com/articles/u-s-agencies-block-technology-exports-for-supercomputer-in-china-1428561987. Access on: Aug. 3, 2022.

CLAUSEWITZ, Carl Von. **On war**. Princeton: Princeton University Press, 1976.

CORERA, Gordon. US warns of supply chain cyber-attacks. **BBC**, London, July 26, 2018. Available at: http://bbc.co.uk/news/technology-44941875. Access on: Aug. 3, 2022.

EPSHTEIN, Uriel; FAINT, Charles. That's logistics: the autonomous future of the Army's Battlefield. *In*: MODERN WAR INSTITUTE. West Point, NY: Modern War Institute, Jan. 2019. Available at: https://mwi.usma.edu/thats-logistics-autonomous-future-armys-battlefield-supply-chain/. Access on: Aug. 3, 2022.

ERICSSON. Press Releases. **Deutsche Telekom and Ericsson strengthen partnership with 5G deal**. Stockholm: Ericsson, 2020. Available at: https://www.ericsson.com/en/press-releases/2020/7/deutsche-telekom-and-ericsson-strengthen-partnership-with-5g-deal. Access on: Aug. 3, 2022.

FREEDMAN, Lawrence. **Strategic coercion**: concepts and cases. Oxford: Oxford University Press, 1998.

FREEDMAN, Lawrence. **Strategy**: a history. Oxford: Oxford University Press, 2015.

GERRING, John. Mere description. **British Journal of Political Science**, [London], v. 42, p. 721-746, 2012. Available at: https://cupdf.com/document/gerring-j-mere-description.html?page=1. Access on: Aug. 3, 2022.

GOODIN, Dan. Cisco confirms NSA-linked zeroday targeted its firewalls for years. **Ars Tchnica**, [California], Aug. 17, 2016. Available at: https://arstechnica.com/security/2016/08/cisco-confirms-nsa-linked-zeroday-targeted-its-firewalls-for-years/. Access on: Aug. 3, 2022.

GRAY, Colin. Why strategy is dificult? *In*: MAHNKEN, T. G.; MAIOLO, J. A. (org.). **Strategic studies**. Oxon: Routledge, 2008. p. 40-47.

GREENWALD, Glenn. **No place to hide**: Edward Snowden, the NSA and the surveillance state. [london]: Penguin Books, 2014.

HALFHILL, Tom R. The truth behind the Pentium Bug. **Byte**, California, Mar. 1995. Available at: https://web.archive.org/web/20060209005434/http://www.byte.com/art/9503/sec13/art1.htm. Access on: Aug. 3, 2022.

HERN, Alex. Oracle in talks with TikTok that could hijack Microsoft bid. **The Guardian**, London, Aug. 2020. Available at: https://www.theguardian.com/technology/2020/aug/18/software-firm-oracle-in-talks-to-buy-tiktok-and-challenge-microsoft-bid. Access on: Aug. 3, 2022.

HOWARD, Michael. The forgotten dimensions of strategy. **Foreign Affairs**, [New York], v. 57, n. 5, p. 975, 1979.

HUTCHINS, Eric M.; AMIN, Rohan M; CLOPPERT, Michael J. **Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains**. [*S. l.*: *s. n.*], 2010. Available at: https://community.mis.temple.edu/mis5208sp2016/files/2015/01/iciw2011.pdf. Access on: Aug. 3, 2022.

JAGODA, Jeneé *et al*. The viability and simplicity of 3D-Printed construction: a military case study. **Infrastructures**, [*s. l.*], v. 5, n. 4, p. 1-10, 2020.

JOMINI, Antoine. **The art of war**. 3. ed. Rockville: Arc Manor, 1862.

KHARPAL, Arjun. US should take stake in Nokia, Ericsson to counter Huawei in 5G: Barr. **CNBC**, [Englewood Cliffs, NJ], 2020.

KRESS, Moshe. **Operational logistics**: the art and science of sustaining military operations. New York: Springer Science+Business Media, 2002.

LEE, Micah; MOLTKE, Henrik. Everybody does it: the messy truth about infiltrating computer supply chains. **The Intercept**, [New York], Jan. 24, 2019. Available at: https://theintercept.com/2019/01/24/computer-supply-chain-attacks/. Access on: Aug. 3, 2022.

LEWIS, James. **Technological competition and China**. Washington, DC: Center for Strategic & International Studies, Nov. 2018. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181130_Technological_Competition_and_China.pdf. Access on: Aug. 3, 2022.

LIDDELL HART, Basil. Economic pressure or continental victories. **Royal United Services Institution Journal**, [London], v. 76, n. 503, p. 486-510, 1931.

LIDDELL HART, Basil. The essence of war. **Royal United Services Institution Journal**, [London], v. 75, n. 499, p. 490-491, 1930.

LIFF, Adam. Cyberwar: a new "Absolute Weapon"? The proliferation of cyberwarfare capabilities and interstate war. **Journal of Strategic Studies**, London, v. 35, n. 3, p. 401-428, 2012. Available at: https://indianstrategicknowledgeonline.com/web/Proliferation%20of%20Cyberwarfare%20Capabilities%20and%20Interstate%20War.pdf. Access on: Aug. 3, 2022.

LEIGHTON, Richard. Logistics: military. *In*: ENCYCLOPAEDIA BRITANNICA. [London]: Encyclopaedia Britannica, 2022. Available at: https://www.britannica.com/topic/logistics-military. Access on: Aug. 3, 2022.

LYNN III, William. Defending a New Domain: the Pentagon's cyberstrategy. **Foreign Affairs**, [New York], v. 89, n. 5, 2010. Available at: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain. Access on: Aug. 3, 2022.

MICROSOFT. Azure. Resources. **What is Middleware?** [Washington, DC]: Microsoft, 2022. Available at: https://azure.microsoft.com/en-us/overview/what-is-middleware/. Access on: Aug. 3, 2022.

MILLER, Greg. How the CIA used Crypto AG encryption devices to spy on countries for decades. **The Washington Post**, Washington, DC, 2020.

MOON, Angela. Exclusive: Google suspends some business with Huawei after Trump blacklist - source. **Reuters**, [Eagan], May 19, 2019. Available at: https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUKKCN1SP0NB. Access on: Aug. 3, 2022.

MORGAN, Patrick. Applicability of traditional deterrence concepts and theory to the cyber realm. *In*: NATIONAL RESEARCH COUNCIL (U.S.). **Proceedings of a workshop on deterring cyberattacks**: informin strategies and developing options for U.S. policy. Washington, DC: National Academies Press, 2010. p. 55-76.

NIST. **Framework for improving critical infrastructure cybersecurity**. [*S. l.*: *s. n.*], 2014. Available at: papers2://publication/uuid/DD40979D-D391-4678-9601-F14CF1CB8BF5. Access on: Aug. 3, 2022.

NIST; FIREEYE. **Best Practices in Cyber Supply Chain Risk Management**. [California]: National Institute of Standards and Technology, 2015. Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-best-practices-in-cyber-supply-chain-risk-management.pdf. Access on: Aug. 3, 2022.

NYE JR, Joseph. Deterrence and dissuasion in cyberspace. **International Security**, [*s. l.*], v. 41, n. 3, p. 44-71, 2017.

PECK, Helen. Supply chain vulnerability, risk and resilience. *In*: WATERS, D. (org.). **Global logistics**: new directions in supply chain management. 6th ed. [*S. l.*]: Kogan Page, 2012. p. 192-207.

PETZINGER, Jill. Deutsche Telekom describes potential Huawei ban as "Armageddon" scenario. **MSN**, June 17, 2020. Available at: https://www.msn.com/en-gb/money/technology/deutsche-telekom-describes-potential-huawei-ban-as-armageddon-scenario/ar-BB15BxQM. Access on: Aug. 8, 2020.

PROENÇA JÚNIOR, Domício; DUARTE, E. E. The concept of logistics derived from clausewitz: all that is required so that the fighting force can be taken as a given. **Journal of Strategic Studies**, [London], v. 28, n. 4, p. 645-677, 2005. Available at: https://www.icesi.edu.co/blogs/estrategialogistica122/files/2012/08/the-concept-of-logistic-derived-from-clausewitz.pdf. Access on: Aug. 3, 2022.

ROGERS, Chairman Mike Rogers; RUPPERSBERGER, Dutch. **Investigative report on the U.S. National security issues posed by Chinese telecommunications companies Huawei and ZTE**. Washington, DC: U.S. House of Representatives, Oct. 2012. Available at: https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf. Access on: Aug. 3, 2022.

ROSA, Bruno; ANTUNES, Cláudia. Embaixador dos EUA alerta que se Brasil permitir chinesa Huawei no 5G enfrentará "consequências". **O Globo**, Rio de Janeiro, jul. 29, 2020. Available at: https://oglobo.globo.com/economia/embaixador-dos-eua-alerta-que-se-brasil-permitir-chinesa-huawei-no-5g-enfrentara-consequencias-24555785. Access on: Aug. 3, 2022.

SANGER, David; PERLROTH, Nicole. FBI Confirms DarkSide as Colonial Pipeline Hacker. **The New York Times**, New York, May 10, 2021. Available at: https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html. Access on: Aug. 3, 2022.

SCHWAAR, Carolyn. U.S. Military To 3D print its way out of supply chain woes. **Forbes**, Feb. 27, 2022. Available at: https://www.scmp.com/business/article/3011377/china-offers-five-year-tax-breaks-chip-makers-software-developers-bolster https://www.forbes.com/sites/carolynschwaar/2022/02/27/us-military-to-3d-print-its-way-out-of-supply-chain-woes/?sh=316b8598275d. Access in: Aug. 4, 2022.

SHERMAN, Mark. **Growing risks in the software supply chain**: Platform Security Summit 2019. [*S. l.*]: Software Engineering Institute; Carnegie Mellon Univerty, Oct. 2019. Available at: https://www.platformsecuritysummit.com/2019/speaker/sherman/PSEC2019-Risks-Software-Supply-Chain-Mark-Sherman.pdf. Access in: Aug. 4, 2022.

SHIDONG, Zhang. China offers five-year tax breaks to chip makers, software developers to bolster industry as trade war stretches to tech. **South China Morning Post**, Shanghai, May 22, 2019. Available at: https://www.scmp.com/business/article/3011377/china-offers-five-year-tax-breaks-chip-makers-software-developers-bolster. Access in: Aug. 2, 2022.

STONE, John. Technology and war: a trinitarian analysis. **Defense & Security Analysis**, [London], v. 23, n. 1, p. 27-40, 2007.

STRUMPF, Dan. Huawei's 5G dominance threatened by U.S. Policy on Chips. **The Wall Street Journal**, New York, 2020. Available at: https://www.wsj.com/articles/huawei-struggles-to-escape-u-s-grasp-on-chips-11592740800. Access in: Aug. 2, 2022.

SUPPLY chains are undergoing a dramatic transformation. **The Economist**, New York, p. 1-7, July 11, 2019. Available at: https://www.economist.com/special-report/2019/07/11/supply-chains-are-undergoing-a-dramatic-transformation. Access in: Aug. 2, 2022.

TOP500.ORG. Lists. **Top500 June 2020**. Sinsheim: Top500.org, 2020. Available at: https://www.top500.org/lists/top500/2020/06/. Access in: Aug. 2, 2022.

TRUMP, Donald J. Executive Order on securing the information and communications technology and services supply chain (EO15873). *In*: THE WHITE HOUSE. Washington, DC: The white House, May 15, 2019. Available at: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/. Access in: Aug. 2, 2022.

TURNBULL, Benjamin. Cyber-resilient Supply chains: mission assurance in the future operating environment. **Australian Army Journal**, [Canberra], v. 14, n. 3, p. 41-56, 2018. Available at: https://search.informit.org/doi/pdf/10.3316/informit.344417545553155. Access on: Aug. 1, 2022.

TZU, Sun. **The Art of War (Restored Translation)**. [*S. l.*]: Pax Librorum, 2009.

UNITED STATES. Defense Logistics Agency. **Defense Logistics Agency strategic plan 2015-2022**. [Virginia]: Defense Logistics Agency, 2015. Available at: https://www.dla.mil/Portals/104/Documents/Headquarters/History/StrategicPlans/2015%20-%202022%20Strategic%20Plan.pdf. Access on: July 28, 2022.

UNITED STATES. Department of Commerce. **Announces the addition of Huawei Technologies Co. Ltd. to the entity list**. Washington, DC: U.S. Department of Commerce, 2019. Available at: https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd. Access on: Aug. 4, 2022.

UNITED STATES. Department of Defense. **Department of Defense Additive Manufacturing Strategy**. Washington, DC: Department of Defense, Jan. 2021a. Available at: https://www.cto.mil/wp-content/uploads/2021/01/dod-additive-manufacturing-strategy.pdf. Access on: Aug. 4, 2022.

UNITE STATES. Department of Defense and General Services Admnistration. **Improving cybersecurity and resilience through acquisition**: final report of the Department of Defense and General Services Admnistration. [Washington, DC: Department of Defense and General Services Admnistration], Nov. 2013a. Available at: https://www.gsa.gov/cdnstatic/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION.pdf. Access on: Aug. 3, 2022.

UNITED STATES. Department of Defense. Defense Science Board. **Cyber supply chain**. Washington, DC: Defense Science Board, 2017.

UNITED STATES. Department of Defense. Defense Science Board. **Resilient Military systems and the advanced cyber threat**. Washington, DC: Defense Science Bord, 2013b. (Task force report). Available at: https://apps.dtic.mil/sti/pdfs/ADA569975.pdf. Access on: Aug. 4, 2022.

UNITED STATES. Department of Defense. **Department of Defense Strategy for Operating in cyberspace**. Washington, DC: Department of Defense, July 2011. Available at: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. Access on: Aug. 4, 2022.

UNITED STATES. Department of Defense. **DoD Open Source Software (OSS) FAQ**. Washington, DC: Department of Defense, Out. 28, 2021b. Available at: https://dodcio.defense.gov/open-source-software-faq/. Access on: Aug. 4, 2022.

UNITED STATES. Department of Defense. Securing Defense-Critical Supply Chains: an action plan developed in response to President Biden's Executive Order 14017. Washington, USA: Department of Defense, Feb. 2022a. Available at: https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF. Access on: Aug. 4, 2022.

UNITED STATES. Department of Treasury Policy issues. International. **The Committee on Foreign Investment in the United States (CFIUS)**. Washington, DC: US Department of the Treasury, [2022b]. Available at: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius. Access in: Aug. 2, 2022.

UNITED STATES. **Foreign economic espionage in cyberspace**. [*S. l.*: *s. n.*], 2018.

VEGETIUS, Flavius Renatus. **De Re Militari**. [*S. l.*: *s. n.*], 1767.

WILLETT, Marcus. Lessons of the SolarWinds Hack. **Survival**, [London], v. 63, n. 2, p. 7-26, 2021.

WOOD, Donald F. Logistics: business. *In*: ENCYCLOPAEDIA BRITANNICA. [London]: Encyclopaedia Britannica, 1998. Available at: https://www.britannica.com/topic/logistics-business. Access on: Aug. 3, 2022.

WOODS, Beau; BOCHMAN, Andy. **Supply chain in the software era**. Washington, DC: Atlantic Council, May 2018. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/supply-chain-in-the-software-era/. Access on: Aug. 1, 2022.

YANG, Yuan; LIU, Nian. Beijing orders state offices to replace foreign PCs and software. **Financial Times**, [London], Dec. 8, 2019. Available at: https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406. Access on: Aug. 1, 2022.

ZETTER, Kim. **Countdown to Zero Day**: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown, 2015a.

ZETTER, Kim. Everything we know about Ukraine's Power Plant Hack. **Wired**, Boone, IA, Jan. 28, 2016. Available at: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/. Access on: Aug. 1, 2022.

ZETTER, Kim. Suite of sophisticated NationState attack tools found with connection to Stuxnet. **Wired**, boone, IA, Feb 16, 2015b. Available at: https://www.wired.com/2015/02/kapersky-discovers-equation-group/. Access on: Aug. 1, 2022.

ECEME