DOI: 10.53477/1842-9904-25-24

CYBERSECURITY SYNERGIES IN LOGISTICS: ADDRESSING THREATS ACROSS CIVILIAN AND MILITARY DOMAINS

Daniela-Elena HRAB* [*]

Current and anticipated developments in logistics focus on implementing a range of emerging technologies that promise substantial economic, social, and environmental advantages. However, these technological innovations also give rise to cyber vulnerabilities that pose significant risk of disruption within supply chains, in the context of a low level of awareness. This study addresses this research problem by investigating such vulnerabilities within the specific context of logistics as a domain shared between civilian and military sectors. The article's research niche lies in its examination of cybersecurity risks at the intersection of civil and military logistics, aiming to identify opportunities for cooperation to mitigate these threats. The study employs a literature review methodology to achieve its objectives. By analysing the cybersecurity implications for civilian logistics and supply chain management first, and then examining the most vulnerable functional and related areas of military logistics, the study adopts a complementary perspective that integrates logistics and cybersecurity. The findings highlight ten key areas of civil-military collaboration, underlining the necessity of a paradigm shift in the delivery of logistic support to military forces, especially in military procurement and operational planning processes.

Keywords: *logistics; military; cybersecurity; procurement; operational planning.*

[*] ***Lieutenant Colonel Daniela-Elena HRAB is an Advanced Military Instructor and PhD Candidate within the "Carol I" National Defence University in Bucharest, Romania. E-mail: edaniela.hrab@gmail.com***

Introduction

The logistics sector is progressively adopting digital solutions to enhance operational efficiency. In 2020, the World Economic Forum projected that digitization could contribute up to $1.5 trillion for the sector by 2025. Among the innovations driving this transformation are technologies such as warehouse robotics, electro-mobility, artificial intelligence/AI, Blockchain, predictive maintenance, and drone supervision. While these technologies offer considerable benefits, these also produce vast quantities of data, thereby increasing the sector's exposure to cybersecurity threats – a risk exacerbated by a persistent deficit in cybersecurity awareness (Prabhughate 2020, 3-4). Prior research indicates that the willingness of logistics managers to implement cyber resilience strategies is significantly influenced by their perception of cyber risks (Gaudenzi and Baldi 2024, 99-122), thereby underscoring the imperative for increased awareness and an integrated focus on both physical and cybersecurity dimensions (Chan and Choi 2023, 1-18).

Military logistics faces similar threats, with China investing in targeting US civilian and military logistics. Such actions pose a significant risk to the operational readiness and responsiveness of NATO forces However, the rapid pace of technological advancement also presents opportunities to develop effective countermeasures. (US Army Futures Command n.d., 8-12). Therefore, identifying cyber threats and fostering military-civil cooperation is critical to enhancing cybersecurity resilience across both sectors.

More than 20 emerging and disruptive technologies have been identified as influencing military cybersecurity, including AI, machine learning/ML, advanced materials, and quantum technologies (NATO Science & Technology Organization 2020, 41-111). Additional relevant technologies include data storage systems, 5G networks, and advanced sensor systems, etc. (Bellasio and Silfversten 2020, 88-108). By 2030, NATO member states are expected to implement private and hybrid 5G networks to support logistics operations in areas such as maintenance, transportation, and training (Pernik 2022, 67). Given this technological landscape, it is imperative for military logisticians to remain informed about developments in both logistics and cyber domains, as cyber threats have the potential to disrupt supply chains and undermine the sustainability of military operations. Within this context, the study addresses the following research problem: a low level of awareness regarding cyber threats and their potential to disrupt supply chain, thereby jeopardizing the continuity and effectiveness of military operations.

Logistics functions differ significantly between civilian and military contexts. In the civilian sector, logistics primarily encompasses transportation, warehousing, and distribution, while Supply Chain Management/SCM include activities such as procurement, production planning, and demand management (Mentzer, Stank and

Esper 2008, 32-35). In contrast, military logistics is considerably broader, comprising six functional areas: the supply of various categories of goods, materiel life-cycle support, equipment maintenance, movement and transportation, general support services (including catering, accommodation, warehousing, laundry and sanitation, postal and courier services, equipment recovery, etc.), as well as medical and veterinary support. Additionally, six related areas are being added, namely: budget and finance, military engineering, mortuary affairs, contractor support to operations, civil-military cooperation and military police functions (NATO Standardization Office 2018, 5_1-6_5). This broader scope highlights that military logistics not only incorporates but extends beyond the functions of civilian logistics and SCM. Accordingly, the objective of this study is to identify and pinpoint potential areas for civil-military collaboration aimed at mitigating cyber risks and improve the sustainability of military operations.

1. Literature Review

The existing body of research on cyberattacks within the logistics sector do not differentiate between civilian and military actors. For instance, Microsoft reported a ransomware attack, allegedly orchestrated by the Russian military operatives, targeting Ukrainian and Polish logistics organizations supporting frontline operations (Lyngaas 2022). Despite the significant impact, limited information was made public, resulting in significant awareness gaps. Consequently, cyber threats to logistics have not been prioritized as a key research area by military logistics experts in at least one of the affected countries over the next five-year period (Jałowiec and Grala 2022, 8-12).

Additionally, research combining cybersecurity and logistics is limited, possibly due to insufficient data highlighting its importance, as most studies address cybersecurity within the broader context of Supply Chain Management (SCM), often overlooking the distinct challenges faced by logistics operations (Cheung, Bell and Bhattacharjya 2021, 1-12). At the same time, logistics often falls under SCM, where continuity of supplies is a key focus (Dymyt, Wincewicz-Bosy and Skubisz 2024, 187), attracting more research interest.

Cybersecurity within logistics and SCM encompasses a broad spectrum of domains, including management, engineering, and operations (Cheung, Bell and Bhattacharjya 2021, 2), rarely considering military contributions. Therefore, military logistics studies often lack detailed analyses of cyber vulnerabilities, missing opportunities to address these through civil-military collaboration. Similarly, civilian-focused research overlooks the potential for military contributions. As a result, military managers lack insights into leveraging civilian expertise to enhance cybersecurity, and civilian sectors miss opportunities for military support. This study aims to bridge this gap by exploring joint civil-military initiatives to bolster logistics cybersecurity in both domains.

2. Research methodology

To achieve the stated objective, the research employs a qualitative strategy grounded in a literature review approach, using the military logistics functional and related areas framework to identify key stakeholders and potential cooperation opportunities. This qualitative method is particularly appropriate as it covers an interdisciplinary topic, enabling preliminary exploration within the intersecting fields of cybersecurity and logistics. Through its characteristics, this strategy allows the applicability of "understanding as a discovery principle" and "the construction of reality as a basis" (Kuckartz and Rädiker 2023, 5).

Moreover, the qualitative strategy aligns well with the exploratory focus of the research goal, which does not aim to test hypotheses (Creswell J.W. and Creswell J.D. 2018, 40, 192). The study adopts an interpretive stance (Denzin and Lincoln 1994, 2), exploring cybersecurity in civilian logistics and SCM, and using a deductive approach to pinpoint areas where military expertise can enhance civilian operations. Furthermore, it analyses military logistics through a comparative approach, highlighting best practices and potential contributions to civilian efforts. As a result, the research offers a holistic view on the issue by analysing various components of military logistics (Creswell J. W. 1998, 15).

3. Cybersecurity Implications for Civilian Logistics and Supply Chain Management

Addressing cybersecurity threats in civilian logistics and SCM is increasingly critical, particularly in the context of Industry 4.0 developments. Emerging technologies such as Blockchain play a key role in safeguarding data generated in logistics by other technologies (Boyson 2014, 2) while also fostering innovation (Tang and Veelenturf 2019, 1-11). Cyber-physical systems/CPS, data science applications (Muhuri, Shukla and Abraham 2019), drones and robots further optimize logistics operations (Cheung, Bell and Bhattacharjya 2021, 13). Despite these benefits, such technologies also increase vulnerability to a range of risks: physical disruptions (e.g., accidents or natural disasters) and cyberattacks, leading to both tangible consequences (reduced production, labour disruptions) and intangible damages, including loss of consumer trust or reputational harm (Chen and Chang 2021, 2-13).

Implementing precautionary measures is essential, beginning with the identification of system vulnerabilities and involving the Chief Information Officer (CIO) to mitigate risks in both information technology/IT and supply chain operations (Cheung, Bell and Bhattacharjya 2021, 5-7). High-profile cyberattacks, such as the attacks on Colonial Pipeline and SolarWinds – underscore the CIO's dual role in ensuring cybersecurity across a broad spectrum of logistics activities, ranging from the supply of everyday products to the acquisition of advanced assets like fighter aircrafts (Dury and O'Meara 2021). Effective measures include implementing blockchain technology, multi-factor authentication (Zhang et al. 2020, 1187-91), installation of secure firewalls and gateways (Hutchins et al. 2015), conducting supplier audits, training personnel (Cheung, Bell and Bhattacharjya 2021, 7-8), and implementing safeguards against counterfeit products (Eggers 2020, 880-5).

Experts highlight that civil-military teams can coordinate three key real-time recovery measures: component recovery, system isolation, and continuous monitoring (Cheung, Bell and Bhattacharjya 2021, 8). In the event of a cyberattack, recovery efforts may also require engaging managers responsible for logistics, procurement, and customer service (Chopra 2018, 1-528).

Aftermath measures often involve CIO-led teams and include behavioural analysis and feedback loops (Sepulveda and Khan 2017, 1293-5), data backups, recovery planning, resilient system design (Colicchia, Creazza and Menachof 2019, 215-40), forensic investigations (Tuptuk and Hailes 2018, 93-106), and system restoration activities (Heath, Mitchell and Sharkey 2020, 5-19). Collaborative recovery strategies often require coordination with supply chain partners (Colicchia, Creazza and Menachof 2019, 221) and insurance providers (Boyson 2014, 9). Additionally, if military supply chains are affected or contractual agreements are in place, military experts may be called upon to support recovery efforts.

Integration sustainability specific to sustainable development in logistics requires strong cybersecurity measures to prevent supply chain disruptions. While technologies such as Blockchain, AI, the Internet of Things (IoT), and Big Data Analytics support this integration, they also heighten vulnerability to cyber threats. Mitigation strategies include the use of Machine Learning (ML) and Cyber Threat Intelligence, while effective implementation requires coordinated efforts among decision-makers, governmental bodies, industry stakeholders, academic institutions, and specialized military personnel in logistics, cybersecurity, and intelligence (Layode et al. 2024, 1954-73).

Maritime logistics, in particular, also presents significant risks, with ports targeted for espionage, terrorism, and cyber warfare, threatening both civilian and military operations. Recommended countermeasures include training, IT infrastructure upgrades, and cooperation with government and international entities (Senarak 2021, 20-36).

Emerging technologies such as Cyber-Physical System (CPS) and Complex Event Processing are increasingly bridging logistics and cybersecurity by enabling real-time data analysis and threat detection (Alias et al. 2018, 1-4). Military logistics could benefit from adopting these innovationss through enhanced cooperation with private companies and the development of smart logistics solutions, addressing risks across personnel, operational processes, and technologies. Recommended measures include network segmentation, rigorous device testing, and AI-based threat monitoring, paired with encryption and employee cybersecurity training programs (Prabhughate 2020, 4-6).

This analysis highlights opportunities for military engagement in addressing logistics cybersecurity, setting the stage for tailored strategies to military operational frameworks.

4. Cybersecurity Implications for Military Logistics

Military logistics is a cornerstone of the broader logistics sector, defined by key domains outlined in NATO standards. These include functional areas such as supply, materiel life cycle support, equipment maintenance, transportation, and medical support, alongside logistics related areas such as finance, engineering, contractor support to operations, and civil-military cooperation (NATO Standardization Office 2018, 5_1-A_1). Additionally, some researchers further emphasize the importance of operational processes, stocks, and technical components, particularly within supply, transport, and services (Brzeziński 2024, 144).

Given the susceptibility of military logistics to cyberattacks, this section explores threats across these domains and explore collaborative countermeasures involving both military and civilian actors. This approach is vital as supply chains underpinning military and civilian logistics share a common structure based on four lines of logistical support. The fourth tier -which includes national depots, contractors, and industrial partners - serves as the strategic foundation for the others (NATO Standardization Office 2018, 1_8). Therefore, cyber threats aiming at civilian logistics can have cascading effects on military supply chains, which may themselves become direct targets.

Research highlights specific vulnerabilities within military supply chains, especially concerning weapon systems, which function as intricate systems-of-systems. These systems are prone to cyberattacks, partly due to flaws in their integrated circuits (Koch and Golling 2016, 192). Additionally, the outsourcing of production to Asia for cost-efficiency has introduced additional risks, such as unauthorized access via backdoors and kill switches in externally manufactured chips, compromising highly classified systems (Adee 2008, 34-9).

Furthermore, cyber risks in military logistics remain persistent due to issues like counterfeit components in naval assets (United States Government Accountability Office 2016, 11-12) and challenges maintaining supply sources for aging weapon platforms. Additionally, the use of commercial off-the-shelf products introduces cyber vulnerabilities, while the integration of legacy systems with modern technologies can create weak points capable of compromising entire military operations (Koch and Golling 2016, 193-5).

Researchers stress that effective cybersecurity begins with the assumption that systems may already be compromised. This requires identifying critical components and implementing risk management practices guided by international standards such as ISO 31000 and IEC 31010 (Koch and Golling 2016, 198). To reduce risks, military logisticians must adopt advanced technologies within their supply chains, develop reliable methods to detect counterfeit parts, and create migration strategies for bridging incompatible systems, with input from civilian and military cybersecurity experts. In parallel, strengthening chip production and supporting EU industrial alliances in semiconductor technologies development are also key priorities (European Commission 2021, 14).

Cyberattacks on civilian supply chains, such as those impacting Colonial Pipeline and JBS Foods, highlight vulnerabilities that could also jeopardize military operations, especially when contractors are involved. Medical support systems face similar threats; for instance, cyberattacks on civilian hospitals as seen in Ireland can hinder healthcare services for both civilian and military patients due to the interconnected nature of their medical infrastructures (NATO 2019, 1_19-1_22). To address these risks, military logisticians should diversify contractors for critical supplies, ensure timely software updates, and foster collaboration between military and civilian sectors. Coordinated efforts are essential to strengthen logistical resilience against cyber threats (NATO Cooperative Cyber Defence Centre of Excellence 2022, 2-4). Furthermore, cybersecurity responsibilities must be clearly assigned across the supply chain, especially for manufacturers, distributors, and importers of digitally integrated products, particularly in information and communication technology. These actors must proactively assess cyber risks, mitigate threats, and comply with conformity assessment procedures to reinforce overall supply chain security (European Commission 2022, 1-17).

In the domains of equipment maintenance and materiel life-cycle support, cybersecurity risks are closely linked to Additive Manufacturing technology. Already adopted by the U.S. military, it enables on-site production of parts, thereby reducing logistical strain and advancing sustainability objectives (Hrab and Minculete 2023, 130). Addressing these risks requires coordinated efforts among 3D printer manufacturers, software developers, equipment suppliers, procurement teams, and military maintenance units.

Similarly, the movement and transportation of military assets are also vulnerable to cyber threats. The U.S. Transportation Command depends heavily on commercial transportation providers and civilian infrastructure - including roads, ports, railways, and electrical grids - to deploy approximately 90% of its troops and equipment. However, these systems lack military protection, leaving critical deployment capabilities exposed to cyber risks (The Brookings Institution 2023, 3-7).

Enhanced military involvement is essential to safeguard critical networks from cyberattacks and economic coercion. For example, China's integrated digital platform for military and civilian entities, connecting 70 ports and more than ten airports, enables coordinated cyber operations. This raises significant concerns about national sovereignty, as controlling and monitoring port data, including entries and departures, may lead to the unintended transfer of operational authority in exchange for assured access (The Brookings Institution 2023, 8).

Furthermore, the military's growing interest in using drones to transport essential supplies, such as petroleum, highlights the need for strong cybersecurity. These autonomous systems require robust cybersecurity to prevent malicious interference. One potential threat scenario involves cyberattacks rerouting autonomous commercial vessels, causing maritime congestion that could obstruct naval operations (U.S. Army Futures Command n.d., 8-9). As adoption of autonomous systems in military mobility depends on IT Systems, smart railroads, and harbours, which heavily rely on GPS (Pernik 2022, 74), the cybersecurity dimension becomes essential.

The EU and NATO acknowledge the critical role of cybersecurity in ensuring effective military mobility. A project under the Permanent Structured Cooperation (PESCO) framework highlights mitigating cyber threats through collaboration between public and private sectors during deployment phases. Key logistical factors, include port accessibility, bridge load capacity, and tunnel dimensions for transporting heavy equipment, and are central to these efforts (Beckvard and Zotz 2021, 1).

Essential for logistic support, critical infrastructure also relies on technology systems, ensuring cybersecurity is imperative. Military logistics platforms, including LOGFAS and warehouse management tools, must also be secured. As a proactive measure, mapping the interdependencies between civilian and military systems is a crucial precautionary step (Beckvard and Zotz 2021, 2). Planners should focus on identifying critical infrastructure and information systems for each operation, and evaluating the risk of potential cyberattack disruptions in both departure and host nations. Additionally, building partnerships to enhance cybersecurity and using Information Sharing and Analysis Centres can foster cooperation and trust. Within the Mission Assurance Process, adopting cybersecurity standards such as ISO/IEC 27001 or the U.S. NIST Cybersecurity Framework is key to establishing a secure operational environment (Beckvard and Zotz 2021, 2-4).

Warehousing is another area vulnerable to cyber threats. Cyberattacks, such as denial-of-service/DoS or database manipulation can disrupt storage facilities by altering product data, especially when systems like Radio Frequency Identification or cellular data are used. Man-in-the-middle attacks pose additional risks by potentially exposing sensitive logistical data to unauthorized entities. Mitigation strategies include securing automated systems, maintaining regular backups, performing routine audits, and providing comprehensive staff training (Beckvard and Zotz 2021, 4).

In the domain of movement and transportation, several aspects need to be thoroughly addressed. First, heavy equipment transport often relies on sea routes using private contracted ships, which are susceptible to cyber disruptions via internet-connected systems. Such cyber threats can delay or obstruct essential deliveries. According to researchers, military planners should engage private companies early in the planning process and mandate adherence to the International Maritime Organization's guidelines on maritime cyber risk management (Beckvard and Zotz 2021, 4). They also stress the need for a robust international legal framework to more effectively address these threats (Al Ali, Chebotareva and Chebotarev 2021, 248).

Secondly, inland waterway transport is exposed to cybersecurity risks similar to those facing maritime transport, River Information Systems and IT infrastructure making these networks attractive targets for cyberattacks (Benga, et al. 2019, 248-50). Any disruption to traffic control could cause cascading effects, such as waterway congestion and broader supply chain interruptions (Beckvard and Zotz 2021, 6).

Thirdly, air transport also faces substantial cyber risks. Military aircraft, much like their civilian counterparts, depend on navigation and air traffic control management systems that ae vulnerable to cyberattacks, including potential breaches in Air Traffic Management systems. Mitigation strategies include establishing alternative flight routes, protection via Military Computer Emergency Response Teams, and coordinating closely with civilian aviation authorities (Beckvard and Zotz 2021, 5-7).

Fourthly, rail transportation is at risk due to its increasing reliance on digital systems like Advanced Train Control Systems, which are susceptible to eavesdropping, spoofing, and denial-of-service (DoS) attacks (Xiang et al. 2020, 46). Addressing these vulnerabilities requires thorough risk assessment during operational planning process/OPP (Beckvard and Zotz 2021, 8).

Seaport cybersecurity plays a vital role in military operations, as ports are integral components to the Joint Logistic Support Network/JLSN, alongside airports and rail ports (NATO Standardization Office 2018, 1_6). Vulnerabilities in systems such as Vessel Traffic Services and cargo handling processes require the deployment of rapid response teams of military personnel, port authorities, and contractor representatives, with joint training and awareness efforts such as infographics and pocket guides. Military mobility, reliant on aerial assets, requires civilian and military cooperation to adopt such measures and embed them within the Operational Planning Process (OPP) (Beckvard and Zotz 2021, 5).

Last but not least, road transportation is essential for military exercises and operations, yet it remains susceptible to threats like attacks on traffic light systems, which can cause congestion that disrupts deployments (Zhiyi et al. 2016, 60-68).

Cities, as part of the JLSN, host key facilities such as hospitals, depots, and convoy support centres (NATO Standardization Office 2018, 1_6). However, the advent of smart cities – where technology is embedded into infrastructure, such as traffic management, energy grids, and healthcare systems – introduces new cyber vulnerabilities. Such threats could disrupt military planning and logistics, highlighting the need for strong collaboration between military leaders and city administrations to implement "security by design" principles into public procurement processes (Bellasio and Silfversten 2020, 111-120).

In this complex landscape, national regulations often fall short in addressing cross-border cyber threats. Effective solutions include mapping vulnerabilities, updating policies and legal frameworks, implementing standards, and fostering agreements among stakeholders to ensure a secure cyber environment (Beckvard and Zotz 2021, 8-9).

Another key area of military logistics highly vulnerable to cyberattacks is contractor support for operations. When responsibilities are outsourced, cybersecurity risks shift to private entities; nonetheless, military logisticians must ensure these risks are effectively addressed. For example, in Japan, defence procurement entities require cyber risk assessments and supplier to comply with cybersecurity standards, including audits and secure supply chains (*Apud* Kono and De Tomas Colatin 2023, 15-16).

In the United Kingdom, Ministry of Defence contractors are required to adhere to the Cyber Security Model, including risk assessments, questionnaires, and evaluations applied to both contracts and subcontracts. However, many contractors face challenges with cloud service and software providers due to the lack of certification and audit standards, underscoring the need for government action and a stronger regulatory framework (UK Government 2021, 3).

The USA has taken a stricter approach, banning high-risk equipment and services from companies such as Huawei, Kaspersky, and ZTE in military contracts, along with restrictions on import and export activities (Federal Communications Commission 2024). Experts advocate for proactive international regulatory frameworks to strenghten supply chain cybersecurity before attacks can occur (Kono and De Tomas Colatin 2023).

5. Main Findings

The analysis highlights key logistics activities across military and civilian domains vulnerable to cyber threats, emphasizing the need for strong collaboration. It also outlines practical solutions achievable through joint efforts involving both logisticians and cybersecurity experts. As a result, ten collaboration areas between military and civilian stakeholders have been identified and are illustrated in Figure no. 1.

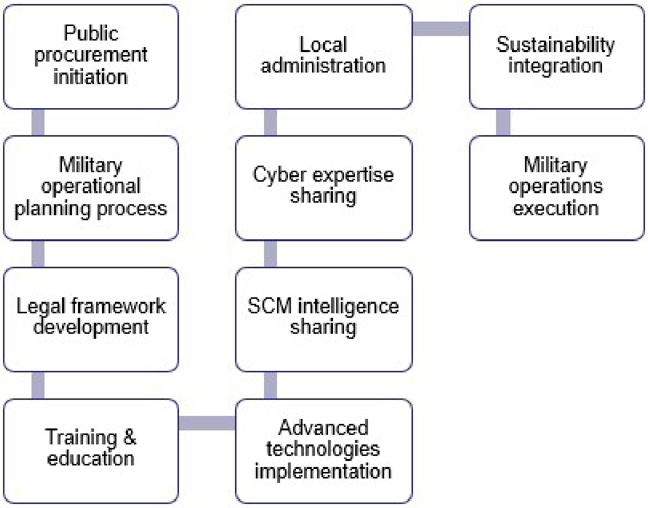
Public procurement initiation
Military operational planning process
Legal framework development
Training & education
Local administration
Cyber expertise sharing
SCM intelligence sharing
Advanced technologies implementation
Sustainability integration
Military operations execution

Figure no. 1: Areas of civilian-military cooperation for cybersecurity in logistics

Conclusions

The current landscape in both military and civilian logistics is increasingly complex and exposed to significant cyber vulnerabilities. Although these sectors are interconnected, the military sector demonstrates a higher level of dependency on secure and resilient logistics. However, logisticians alone cannot address the challenges posed by technology integration and cyber threats to logistic support. Therefore, in the military sector, the success of operations and missions hinges on the establishment of interdisciplinary teams. These teams should include civilian and military logisticians, IT and cyber experts, representatives from producers, contractors, intelligence agencies personnel, administrative authorities, academic researchers, and other key stakeholders to effectively address cyber vulnerabilities across the ten identified areas of collaboration.

Within these interdisciplinary teams, logisticians play a critical role by deconstructing logistics processes into detailed components, enabling the identification of key actors and potential cyber threats. Nonetheless, the input of other team members is essential to ensure, for instance, that procurement processes and operational planning effectively mitigate a wide range of threats that could compromise the supply chain. This approach applies to all functional and related areas of military logistics, whether addressing the need for daily consumables or essential military equipment on the battlefield. Overlooking these considerations, particularly in procurement and operational planning, could render a military force unable to mobilize or sustain operations effectively.

From a procurement standpoint, military structures must expand their focus beyond standard product specifications, delivery terms, and payment conditions. Additional considerations, such as demand forecasting, the creation of a vetted and certified pool of national suppliers subject to military audits and oversight, securing multiple sources for critical products and service, imposing restrictions on the import and export of certain types or components of essential military equipment, and assigning clear cyber responsibilities to contractors, are already proving a significant impact on military procurement practices. Their effectiveness depends on the establishment of a robust legal framework, which can be developed collaboratively and supported through agreements among all relevant stakeholders. Furthermore, a cultural shift within military institutions may be necessary, such as fostering openness and transparency, as these are essential for successful collaboration with third parties.

Incorporating cybersecurity considerations into the operational planning process requires a fundamental shift in perspective, as emphasized in this study. To facilitate this change, several key actions should be prioritized during peacetime and validated through military exercises. These include: integrating cybersecurity into the design, monitoring, protection, and management of public infrastructure; active involvement from private and public sectors; focus on identifying interdependencies across systems; and establishing rapid-response teams to address cyberattacks effectively.

In addition to involving external parties into logistics-related military activities, military actors can also enhance engagement with the civilian sector through initiatives such as: cooperating with local authorities, identifying critical information infrastructure, protecting critical logistic infrastructure, promoting cybersecurity awareness, and providing education and training for both civilian and military logisticians. Additionally, offering cyber expertise to key stakeholders. In fact, education and training in cybersecurity for logistic processes to key stakeholders remains a valuable option. Notably, joint education and training in cybersecurity for logistics represents a strategic priority that can be significantly advanced through military-civilian collaboration.

While the ten areas of civil-military cooperation identified in this study encompass various distinct yet interconnected activities, the effectiveness of cybersecurity in logistics can be achieved through a coordinated and integrated implementation of these actions. Since they are interlinked, failure in one area could have a cascading negative impact on others, underscoring the need for a strategic approach.

Drawing on the insights presented, this study also identifies practical ways to implement cybersecurity measures into logistic practices. One of the most achievable steps is to *raise awareness among logisticians*, encouraging them to look beyond the traditional characteristics of military products and conventional logistics processes. To this end, logisticians should have access to updated training programs that not only address logistics but also highlight the cyber risks associated with its proper functioning. Furthermore, they should be equipped to understand how emerging technologies support logistics operations while simultaneously introducing cyber threats that could compromise military missions and operations.

Another approach to implementing cybersecurity measures in logistics is to establish an organizational habit of consulting cybersecurity experts prior to the procurement of military equipment. These experts can better assess the cybersecurity implications and contribute to refining operational requirements so that technical specifications explicitly address cybersecurity vulnerabilities. It is increasingly clear that merely acquiring equipment is not sufficient to safeguard against supply chain disruptions caused by cyberattacks. While this approach could be formalized through military directives and regulations, its success depends on decision-makers recognizing the negative consequences of maintaining the current modus operandi.

As the defence industry continues to evolve, a third approach to integrate cybersecurity into logistics practices involves engaging interdisciplinary teams – bringing together civilians and military personnel, logisticians and cyber experts, as well as producers and end-users – during the early stages of product design. To support this collaborative effort, a dedicated legal framework should be developed to clearly outline the scope and limits of cooperation between military procurement authorities and industry partners, aligned with the nation's economic capabilities and strategic priorities.

Lastly, military exercises designed to evaluate the resilience of both civilian and military logistics support lines against cyberattacks should be routinely conducted. These exercises can help assess the scale of the problem and identify practical entry points for mitigation, especially given the diversity of equipment and systems used by various armed forces. For nations engaged in military alliances and partnerships, interoperability presents an additional layer of complexity. Therefore, procurement decisions made by one country should be carefully considered by partner nations, and multinational, interdisciplinary teams should be involved to develop the most effective and coordinated responses.

In addition to identifying important areas of civil-military cooperation to address cybersecurity threats to logistic operations and exploring practical ways to implement cybersecurity measures into practice, this article highlights another critical aspect: the need for a comprehensive, in-depth approach when identifying such cooperation opportunities. As such, future studies should focus on identifying common ground in civil-military relations and further exploring potential avenues for joint actions to counter cyber threats.

Acknowledgement: *This study was carried out within the framework of the Strengthening Synergies in Defence and Civilian Cybersecurity - ECYBRIDGE project, funded by the European Union, under Grant Agreement No. 101158784 - DIGITAL-ECCC-2023-DEPLOY-CYBER-04-CIVIL-DEFENCE.*

BIBLIOGRAPHY:

Adee, Sally. 2008. *The hunt for the kill switch. Are chip makers building electronic trapdoors in key military hardware? The Pentagon is making its biggest effort yet to find out.* https://spectrum.ieee.org/the-hunt-for-the-kill-switch (accessed November 5, 2024).

Al Ali, Naser Abdel Raheem, Anna A. Chebotareva, and Vladimir E. Chebotarev. 2021. "Cyber security in marine transport: opportunities and legal challenges." *Scientific Journal of Maritime Research* 35: 248-255. https://hrcak.srce.hr/file/387886

Alias, Cyril, Frank Eduardo Alarcón Olalla, Hauke Iwersen, Julius Ollesch, and Bernd Noche. 2018. "Identifying Promising Application Areas for Cyber-Physical and Complex Event Processing in Logistics Practice." *Logistics* (MDPI) 2, no. 4: 1-24. https://www.mdpi.com/2305-6290/2/4/23

Beckvard, Henrik, and Philippe Zotz. 2021. *Cyber Considerations for Military Mobility.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 1-11. https://ccdcoe.org/uploads/2021/05/Releasable_Cyber-Considerations-for-Military-Mobility_Beckvard_Zotz.pdf

Bellasio, Jacopo, and Erik Silfversten. 2020. "The Impact of New and Emerging Technologies and the Cyber Threat Landscape and Their Implications for NATO'." In *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, by Amy Ertan et al. (eds)., 88–108. CCDCOE.https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis/

Benga, Gabriel Constantin, Ionel Dănuț Savu, Sorin Vasile Savu, Bebe Adrian Olei, and Răzvan Ionuț Iacobici. 2019. "Assesment of Trends in Inland Waterway Transport within European Union.", Advanced Engineering Forum, 34.": 247–254. https://www.researchgate.net/publication/336256544_Assesment_of_Trends_in_Inland_Waterway_Transport_within_European_Union

Boyson, S. 2014. "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems." *Technovation* (Elsevier) 34, no. 7: 342–353. https://www.sciencedirect.com/science/article/abs/pii/S0166497214000194

Brzeziński, Marian Henryk. 2024. "Holistic foundations of military logistics theory development." *Military Logistics Systems* 60: 135-147. https://slw.wat.edu.pl/pdf-193854-114911?filename=114911.pdf

Chan, Hau Ling, and Tsan-Ming Choi. 2023. "Logistics management for the future: the IJLRA framework." *International Journal of Logistics Research and Applications* (Taylor & Francis) 27, no. 12: 1-19. https://www.tandfonline.com/doi/full/10.1080/13675567.2023.2286352

Chen, Li-Ming, and Wei-Lun Chang. 2021. "Supply- and cyber-related disruptions in cloud supply chain firms: Determining the best recovery speeds." *Transportation Research Part E* (Elsevier) 151: 1-18. https://www.sciencedirect.com/science/article/abs/pii/S1366554521001186

Cheung, Kam-Fung, Michael G.H. Bell, and Jyotirmoyee Bhattacharjya. 2021. "Cybersecurity in logistics and supply chain management: An overview and future research directions." *Transportation Research Part E* (Elsevier) 146: 1-18. https://www.sciencedirect.com/science/article/abs/pii/S1366554520308590

Chopra, Sunil. 2018. *Supply Chain Management: Strategy, Planning, and Operation.* Seventh Edition. Pearson Education Limited.

Colicchia, Claudia, Alessandro Creazza, and David Menachof. 2019. "Managing cyber and information risks in supply chains: insights from an exploratory analysis." *Supply Chain Management* (Emerald) 24, no. 2: 215-240. https://doi.org/10.1108/SCM-09-2017-0289

Creswell, J. W., Creswell, J. D. 2018. *Research design: qualitative, quantitative, and mixed methods approaches*. Fifth edition. SAGE Publications Inc.

Creswell, J. W. 1998. *Qualitative Inquiry and Research Design. Choosing among Five Traditions*. Thousand Oaks. SAGE Publications Inc.

Denzin, Norman K., Lincoln, Yvonna S. (*eds.*) 1994. *Handbook of Qualitative Research*. Thousand Oaks, SAGE Publications Inc.

Dury, Jason, and Jack O'Meara. 2021. *The CIO's role in maintaining a strong supply chain. Supply chains are no longer focused wholly on just-in-time delivery and logistics any more than CIOs are focused entirely on help desks and printers.* https://www.ciodive.com/news/cio-supply-chain-tips/605795/.

Dymyt, Małgorzata, Marta Bianka Wincewicz-Bosy, and Oskar Skubisz. 2024. "Global or local - glocalization as a challenge for the modern supply chains management." *Military Logistics Systems* 60: 181-197. https://slw.wat.edu.pl/pdf-193857-114914?filename=114914.pdf

Eggers, Shannon. 2020. "A novel approach for analyzing the nuclear supply chain cyber-attack surface." *Nuclear Engineering and Technology* 53: 879-887. https://www.sciencedirect.com/science/article/pii/S1738573320308573

European Commission. 2022. "Cyber Resilience Act." Brussels, 1-17. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. 2021. "Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery." Brussels,1-23. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1884

Federal Communications Commission. 2024. *List of Equipment and Services Covered by Section 2 of The Secure Networks Act*. https://www.fcc.gov/supplychain/coveredlist.

Gaudenzi, Barbara, and Benedetta Baldi. 2024. "Cyber resilience in organisations and supply chains: from perceptions to actions." *The International Journal of Logistics Management* 35, no. 7: 99-122. https://www.emerald.com/insight/content/doi/10.1108/ijlm-09-2023-0372/full/html

Heath, E.A., J.E. Mitchell, and T.C. Sharkey. 2020. "Models for restoration decision making for a supply chain network after a cyber attack." *The Journal of Defense Modeling and Simulation* (Sage Journals) 17, no. 1: 5–19. https://journals.sagepub.com/doi/full/10.1177/1548512918808410

Hrab, Daniela-Elena, and Gheorghe Minculete. 2023. "Building tomorrow: additive manufacturing unleashing sustainable progress in the US military." *Insights into Regional Development* (Entrepreneurship and Sustainability Center) 5, no. 4: 115-134. https://www.researchgate.net/publication/376797913_Building_tomorrow_additive_manufacturing_unleashing_sustainable_progress_in_the_US_military

Hutchins, M.J., R. Bhinge, M.K. Micali, S.L. Robinson, J.W. Sutherland, and D. Dornfeld. 2015. "Framework for identifying cybersecurity risks in manufacturing." *Procedia Manufacturing 1*: 47–63. https://www.sciencedirect.com/science/article/pii/S2351978915010604

Jałowiec, Tomasz, and Dariusz Grala. 2022 "Research dilemma of military logistics." *Military Logistics Systems* 56: 5-14. https://www.researchgate.net/publication/364080355_Research_dilemma_of_military_logistics

Koch, Robert, and Mario Golling. 2016. "Weapons Systems and Cyber Security – A Challenging Union", in N.Pissanidis, H.Rőigas, M.Veenendaal (Eds.). *8th International Conference on Cyber Conflict: Cyber Power.* Tallinn, Estonia: NATO CCD COE Publications. 191-203. ". https://www.ccdcoe.org/uploads/2018/10/Art-12-Weapons-Systems-and-Cyber-Security-A-Challenging-Union.pdf

Kono, Keiko, and Samuele De Tomas Colatin. 2023. *National Approaches to the Supply Chain Cybersecurity: Taking a More Restrictive Stance Against High-Risk Vendors.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Kuckarts, Udo, and Rädiker, Stefan. 2023. *Qualitative Content Analysis. Methods, Practice and Software.* Second Edition, SAGE Publications Inc., London.

Layode, Oluwabunmi, Henry Nwapali Ndidi Naiho, Talabi Temitope Labake, Gbenga Sheriff Adelek, Ezekiel Onyekachukwu Udeh, and Ebunoluwa Johnson. 2024. "Addressing Cybersecurity Challenges in Sustainable Supply Chain Management: A Review of Current Practices and Future Directions." *International Journal of Management & Entrepreneurship Research* 6, no. 6: 1954-1981. https://www.researchgate.net/publication/383398010_Addressing_Cybersecurity_Challenges_in_Sustainable_Supply_Chain_Management_A_Review_of_Current_Practices_and_Future_Directions

Lyngaas, Sean. 2022. *Microsoft blames Russian military-linked hackers for ransomware attacks in Poland and Ukraine.* Prod. CNN.

Mentzer, John T., Theodore P. Stank, and Terry L. Esper. 2008. "Supply Chain Management and Its Relationship to Logistics." *Journal of Business Logistics* (Wiley) 29, no. 1: 31-46. https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2158-1592.2008.tb00067.x

Muhuri, Pranab K., Amit K. Shukla, and Ajith Abraham. 2019. "Industry 4.0: A bibliometric analysis and detailed overview." *Engineering Applications of Artificial Intelligence* (Elsevier) 78: 218-235. https://www.sciencedirect.com/science/article/abs/pii/S0952197618302458

NATO Cooperative Cyber Defence Centre of Excellence. 2022. "Recent Cyber Events: Considerations for Military and National Security Decision Makers. Reflections on 2021: the ransomware threat, supply chain security, spyware export controls.". https://ccdcoe.org/uploads/2022/02/Report_Reflections_on_2021_A4.pdf

NATO Science & Technology Organization. 2020. "Science & Technology Trends 2020–2040. Exploring the S&T Edge.", 1-160. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

NATO Standardization Office. 2019. "NATO Standard AJP-4.10, Allied Joint Doctrine for Medical Support", Edition C, Version 1. https://www.coemed.org/files/stanags/01_AJP/AJP-4.10_EDC_V1_E_2228.pdf

NATO Standardization Office. 2018. "NATO Standard AJP-4 Allied Joint Doctrine for Logistics". https://assets.publishing.service.gov.uk/media/5f2d4db5d3bf7f1b1b53e80e/doctrine_nato_logistics_ajp_4.pdf

Pernik, Piret. 2022. "Drivers of Change Impacting Cyberspace in 2030." Chap. 5 in *Cyberspace Strategic Outlook 2030. Horizon Scanning and Analysis*, edited by Piret Pernik, 104. Tallinn: NATO CCD COE Publications. https://ccdcoe.org/library/publications/cyberspace-strategic-outlook-2030-horizon-scanning-and-analysis/

Prabhughate, Arati. 2020. *Cybersecurity for Transport and Logistics Industry. View Point.* Infosys Limited, 1-8. https://www.infosys.com/services/cyber-security/documents/transport-logistics-industry.pdf

Senarak, Chalermpong. 2021. “Port cybersecurity and threat: A structural model for prevention and policy development.” *The Asian Journal of Shipping and Logistics* (Elsevier) 37, no. 1: 20-36. https://www.sciencedirect.com/science/article/pii/S2092521220300389

Sepulveda, D. A., and O. Q. Khan. 2017. “A system dynamics case study of resilient response to IP theft from a cyber-attack.” *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).* Singapore: IEEE,1291-1295.https://backend.orbit.dtu.dk/ws/portalfiles/portal/149425868/PID4982587.pdf

Tang, Christopher S., and Lucas P. Veelenturf. 2019. “The strategic role of logistics in the industry 4.0 era.” *Transportation Research Part E: Logistics and Transportation Review* (Elsevier) 129: 1-11. https://www.sciencedirect.com/science/article/abs/pii/S1366554519306349

The Brookings Institution. 2023. *Securing Global Mobility: A Conversation with General Jacqueline Van Ovost, 14th Commander of the US Transportation Command, Webinar*.

The UK Government. 2018. “DCPP Cyber Security Model: Industry Buyer and Supplier Guide.”, 1-30. https://www.gov.uk/government/publications/dcpp-cyber-security-model-industry-buyer-and-supplier-guide

The UK Government. 2021. “Policy Paper: Government Response to the Call for Views on Supply Chain Cyber Security.” *UK Government website.*. https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security (accessed November 5, 2024).

Tuptuk, Nilufer, and Stephen Hailes. 2018. “Security of smart manufacturing systems.” *Journal of Manufacturing Systems* 47: 93-106. https://www.sciencedirect.com/science/article/pii/S0278612518300463

United States Government Accountability Office. 2016. “Report to Congressional Committees, Counterfeit Parts. DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk.”, 1-49. https://www.gao.gov/products/gao-16-236

US Army Futures Command. n.d. “Future Operational Environment: Forging the future in an uncertain world 2035-2050.”, 1-25. https://community.apan.org/cfs-file/__key/telligent-evolution-components-attachments/01-9016-00-00-00-16-09-66/AFC-Pam-525_2D00_2-The-Future-Operational-Environment-2035_2D00_2050.pdf

Xiang, Liu, et al. 2020. *Cyber Security Risk Management for Connected Railroads.* Washington, DC: US Department of Transportation. https://railroads.dot.gov/elibrary/cyber-security-risk-management-connected-railroads

Zhang et al. 2020. “Industrial Blockchain of Things: A Solution for Trustless Industrial Data Sharing and Beyond.” *16th International Conference on Automation Science and Engineering (CASE)*. IEEE, 1187-1192. https://ieeexplore.ieee.org/document/9216817

Zhiyi, Li, Dong Jin, Christopher Hannon, Mohammad Shahidehpour, and Jianhui Wang. 2016. “Assessing and mitigating cybersecurity risks of traffic light systems in smart cities.” *Cyber-Physical Systems: Theory & Applications 1* (IET) 1, no. 1: 60-69. https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-cps.2016.0017