Chapter 3

The Colombian National Army's Logistics Chain, Cybersecurity and Cyber Defense: Attention to Academia*

DOI: https://doi.org/10.25062/9786287818064.03

Sergio Barrios Torres

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: This chapter explores the strategic interest of the Colombian National Army in understanding the relationship among cybersecurity, cyber defense, and military logistics. It emphasizes the urgent need to enhance knowledge in this field, both in academic settings and through updates to military doctrine, to strengthen national security. The chapter also highlights that logistical capabilities supporting military operations hold significant strategic importance while identifying potential conceptual and operational gaps that could lead to vulnerabilities. Lastly, it suggests areas for reflection that can serve as foundational elements for future research and doctrinal advancements aimed at improving and safeguarding the military logistics chain of the Colombian Army from an emerging cybersecurity perspective.

Keywords: supply chain; logistics chain; cyber defense; cybersecurity; strategy; military logistics

* Book chapter resulting from the research project *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* conducted by the Cyberspace, Technology, and Innovation research group of Escuela Superior de Guerra "General Rafael Reyes Prieto," categorized C by the Ministry of Science, Technology and Innovation (MinCiencias) and registered under code COL0181179. The points of view and results of this chapter belong to the authors and do not necessarily reflect those of the participating institutions

Sergio Barrios Torres
Master's in Comprehensive Logistics, Universidad Militar Nueva Granada, Colombia. Specialization in National Security and Defense and Specialization and Certificate Course in Command and General Staff, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Bachelor's in Military Sciences, Escuela Militar de Cadetes "General José María Córdova," Colombia. **https://orcid.org/0000-0001-7207-4605**
Contacto: **sergio.barrios@esdeg.edu.co**

APA Citation: Barrios Torres, S. (2025). The Colombian National Army's Logistics Chain, Cybersecurity, and Cyber Defense: Attention to Academia. In M. E. Realpe Díaz & A. M. González González (Eds.), *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* (pp. 69-98). Sello Editorial ESDEG.
https://doi.org/10.25062/9786287818064.03

DISRUPTIVE TECHNOLOGIES, LOGISTICS, AND NATIONAL SECURITY AND DEFENSE IN CYBERSPACE
Print ISBN: 978-628-7818-05-7
Digital ISBN: 978-628-7818-06-4
DOI: https://doi.org/10.25062/9786287818064

Cybersecurity and Cyber Defense Collection
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Introduction

Military logistics is a sensitive element with the highest impact on the State's security and defense system. This importance is reflected in the intention of the doctrinal update of the Colombian National Army, which emphasizes it as a function that integrates the application of military strategy with the grouping of tasks and systems united by a common purpose, identified as military objectives and support tasks in land military and national defense operations. In this doctrinal update, the tasks of warfighting are highlighted, including sustainment, which involves utilizing systems represented in personnel, knowledge, tasks, and infrastructure that provide support and services to achieve operational objectives that grant the military commander "freedom of action, extending the operational scope, and prolonging resistance" at all levels against threats or the enemy (Fuerzas Militares de Colombia, 2018, p. 66).

In addition to the above, the concept of cyberspace addresses and integrates cybersecurity and cyber defense, defining cyberspace as a complex arena linked to the seamless flow of data transmitted through computer networks. Initially established for military forces (MF), it has since evolved for broader societal use. Consequently, the vulnerabilities inherent in both military and civilian information systems must be understood in today's globalized context, as they can filter, corrupt, or destroy data for political and military purposes. This especially leads to weaknesses or lapses in control over sensitive information, potentially triggering interventions, reaching certainty of capability access, and influencing social behavior through distorted narratives or misinformation (NATO, 2020, pp. 1–2).

The conceptual importance of cyber defense is evident in the statements made by Sánchez (2020), who, citing concepts from the Communications Regulation Commission (CARI, 2009), defines cybersecurity as:

> a set of tools, policies, security concepts, security safeguards, guidelines, risk management methods, actions, training, best practices, insurance, and technologies that can be used to protect organizational assets and users in cyberspace. Cybersecurity ensures that the security properties of assets and users are achieved and maintained against relevant security risks in cyberspace. (p. 35)

Consequently, the performance of cybersecurity is highlighted and defined as

> [...] all the activities necessary for the protection of information networks and systems, the users of such systems, and other people affected by cyber threats, as considered by the European Parliament (2019) and the Council of the European Union, under the work of the European Union Agency for Cybersecurity. (p. 32)

This chapter delves into the strategic interest of the Colombian National Army in studies that establish the crucial link among cybersecurity, cyber defense, and military logistics. It also explores the warfighting function of sustainment, which is why this research aims to formulate reasons for the importance of promoting knowledge within the relevant academic community to enhance specific thematic aspects.

Transformations have occurred in cyberspace that directly impact information security, as evidenced by the increase in preventive measures against cyberattacks, the allocation of resources, the acquisition of equipment, and the development of specialized knowledge. In other words, there is greater technological dependence that escalates threats in the digital realm. Therefore, academia must prioritize strengthening cyber defense and cybersecurity mechanisms, particularly the security of the military logistics chain of sustainment. This requires expanding knowledge about potential threats that may compromise the capabilities, advantages, and disadvantages of the Colombian National Army's operational support system, which serves as a pillar for the defense and security of the State.

Given this concern, the processes of planning and conducting operations require adaptability. This is why it is important to devise real-time military superiority strategies for the various threats that can undermine the expected performance of military logistics in Colombia, particularly due to the lack of understanding of potential weaknesses in defense supply chains.

Cybersecurity, Cyber Defense, and Military Logistics of the Colombian National Army

Many functions and performances of military logistics today rely on computer networks and the management of information and goods flow. Their operation is based on a complex environment that encompasses human capital management, infrastructure, training systems, maintenance of capabilities, stock procurement, and management systems. Additionally, it involves various modes and means of supply and provisioning, which require careful management due to their strategic locations and adaptability to environments defined by their capabilities and the operational context.

Therefore, when the National Army undertakes military defense and security actions, a continually evolving logistics chain has been developed, evolving from simply acquiring goods and services to achieving tactical, productive, administrative, and operational improvements as strategic support. Nowadays, the Army's military logistics bases its performance on access to information technologies. Given this technological dependence, there is an increasing need for the Colombian National Army to remain steadfast and resist all types of computer attacks or cyberattacks that could pose threats or adversaries seeking sensitive information represented in strategic assets, which would demonstrate logistical support and self-sustaining capabilities.

How much can the lack of academic and doctrinal development affect the relationship among *military logistics, cybersecurity,* and *cyber defense* in support of the Colombian National Army's operations? This chapter critically analyzes the pressing need to increase the research and academic focus to support the doctrine that addresses this relationship.

In response to the stated problem and the central question, we establish a general objective that will serve as the common thread for the research. This objective will be achieved through specific interim analyses to promote the optimal development of the research proposal. A path will be pursued to highlight the importance of expanding academic knowledge about the relationship among cybersecurity, cyber defense, and military logistics in the academic, doctrinal, and operational fields of the Army.

Additionally, the scope of analysis and intermediate objectives are outlined. We aim to conceptualize and highlight the significance of the relationship among cyber defense, cybersecurity, and the Army's logistics chain as a crucial factor in its supply chain, thereby enhancing the performance of the sustainment warfighting function (WFF).

Secondly, we evaluate and justify the adoption or consideration of the approach introduced by various means and concepts. This approach underlines the importance of guiding academia in research and the further development of knowledge regarding the relationship between the Army's logistics chain and cybersecurity, serving as a factor for improving the performance of the supply chain, the integrated logistics management system, and, of course, the sustainment WFF.

Moreover, as a final intermediate and specific objective, we aim to conduct an analysis that identifies the strengths, weaknesses, opportunities, and threats related to the Army's logistics and supply chains. This will be based on the growing body of research linking cybersecurity and cyber defense to the Army's logistics chain, with the goal of developing a tool to enhance the efficiency of its supply chain.

Methods

This research employs a qualitative approach and focuses on specific topics within the domain of knowledge: logistics, military logistics, cybersecurity, and cyber defense. Therefore, according to Hernández et al. (2014),

> The initial immersion in the field means becoming aware of the environment in which the study will be conducted, identifying informants who provide data and guide the researcher through the area, penetrating and understanding the research situation, and verifying the feasibility of the study. (p. 8)

Therefore, this analysis employs an inductive approach to examine various conceptual and theoretical perspectives. Data, theories, and a range of opinions are gathered to investigate the central issue and address the key problem question, in accordance with the intermediate objectives. Additionally, the author's experiences and viewpoints are taken into account, along with the contributions of pertinent concepts and opinions. Thus, it is

> postulated that "reality" is defined by research participants' interpretations of their realities. In this way, several "realities"—at least that of the participants, that of the researcher, and that stemming from the interaction of all actors—converge. (Hernández et al., 2014, pp. 8–9)

We propose an approach based on the structured data gathered from open sources, such as research articles and specialized publications related to military logistics, cybersecurity, and cyber defense. This approach comes from the perspective of the author, a specialist in military logistics, aiming to identify valuable information that serves as a foundation for exploration and contextualizes the proposed topic.

In addition, two additional techniques are used: bibliographic-documentary analysis and historical-logical analysis. Bibliographic analysis consists of selecting and collecting information from various sources, such as libraries and documentation centers, to then analyze and present results, thus contributing to the construction of knowledge (Matos, 2020, para. 8).

On the other hand, Rodríguez and Pérez (2017) propose that historical-logical analysis is a method or skill where

> the historical and the logical are closely linked. To discover the essence of the object, the logical requires the data provided by the historical [...]. The logical must reproduce the essence and not limit itself to describing the historical facts and data. These ideas are summarized in that the logical is the historical freed from the historical form [...] The analysis of investigative practice makes it possible to affirm that this method is commonly used when searching for the background of the scientific problem and during the preparation of the theoretical foundations and methods of the proposed solution to the problem [...] its purpose is the search for information as part of the network of inquiries. (pp.189–190)

Therefore, given the accumulation and appropriation of data and documentary management to obtain information deemed relevant, we intend to conduct an information assessment based on principles such as those established by Hitzler and Honer (2016). They argue that the fundamental techniques of qualitative data collection consist of observing events and obtaining documents. Observation serves to gather sensory impressions, create experiences, and record phenomena. Observation approaches should take place during the research process, forming the theories with an upward trend: Observations are specified and systematized in the shape of a funnel (p. 63).

In this way, more than eighty sources were reviewed, including scientific articles and academic and official documents addressing cybersecurity, cyber defense, and military logistics. The most relevant ones for this document were selected and included in the bibliography.

An attempt is made to correlate the information collected with the objectives set, which, as stated by Martínez et al. (2023), is a methodological approach in which the analyst makes a series of decisions to build knowledge, as a systematic and logical sequence is proposed. Soundness is provided in the process, the robustness of scientific evidence, and the researcher's competencies (p. 79). This aims to fulfill the first specific objective.

We propose to emphasize the significance of developing a conceptual approach that examines the relationship among the main themes. A comparative approach is employed to evaluate how cybersecurity and cyber defense impact the performance of military logistics and the Army's supply chain, analyzing their scientific contributions and the similarities and differences in their applications. This mental operation entails observing, analyzing, and interpreting elements that subsequently enable us to generate meanings and produce knowledge (Jiménez Jiménez, 2021, p. 181).

Power factors are compared with multipliers in cybersecurity theories and practices. These conceptual applications and considerations set the objective using a constructivist approach and an observational method to collect simple information and analyze variables. This helps the researcher enrich the document by identifying differences and personal interpretations (O'leary, 2014, as cited in Rodríguez, n.d., pp. 33–35), leading to a stronger rationale for proposing a greater focus on enhancing cyber defense within the supply chain of the integrated logistics management system through doctrinal expansion and research.

Consequently, the third matter highlighted in this investigation and analysis is addressed reflectively through a SWOT analysis. This approach establishes the thematic line and deepens the relationship among cybersecurity, cyber defense, and military logistics in academia, while also allowing for an understanding of the strengths, weaknesses, opportunities, and threats of the Military Forces and what they represent for military strategy, national security, and defense. As discussed by Ponce (2007, pp. 114–117), evaluating the solid and weak factors that diagnose the internal situation of an organization or purpose provides a sample of opportunities and threats. The model to be used is shown in Figure 1.

Figure 1. *SWOT Analysis Matrix*

SWOT ANALYSIS	**Strengths** Own elements to highlight	**Weaknesses** Elements to review/improve
Opportunities External elements that may represent an opportunity	**SO Strategies** Using strengths to take advantage of opportunities	**WO Strategies** Overcoming weaknesses by taking advantage of opportunities
Threats Elements that represent an external advantage and may affect interests	**ST Strategies** Using strengths to avoid threats	**WT Strategies** Minimizing weaknesses and avoiding threats

Source: Own elaboration based on AMCES (2023).

Logistics, Cybersecurity, and Cyber Defense Relationship

Logistics and Military Logistics

The swinging, the dynamics, and the transformation of conflicts, war, and threats today require constant evolution due to the ever-changing nature of our world. The frenetic pace of technological advancement influences the emergence of new ideas, regulations, methods, and tools, which are made available to logistics as instruments in search of the optimal support system for military structures in their state task of providing security and defense.

The origin of comprehensive and business logistics stems from the concern of refining troop movements, accommodation, and support on a large scale, along with the provision of ammunition and supplies necessary for military endeavors. Thus, Baron Jomini, serving Napoleon I and the Tsar of Russia in the 19th century, regarded logistics as one of the three structures to emphasize in the art of war, alongside tactics and strategy (Montanyá, 2021). Consequently, military logistics is defined as part of the science and art of war, and like it, has been integral to human history, evolving and refining until it became a science applicable to various support processes for operational forces. Military logistics is defined as "that part of the art of war that aims to provide the Armed Forces with the necessary means to meet the demands of war adequately" (FAC, 2016, p. 2)

The constant evolution of logistics within the business world imposes new concepts and the creation of global entities focused on its study, such as the Council of Supply Chain Management Professionals (CSCMP, 2023), which currently advocates for collaboration among supply chain management professionals worldwide by promoting appropriate education and development in logistics.

The doctrinal update of the Colombian National Army states that, although military logistics as a concept does not disappear, it does prominently and evolutionarily introduce an action largely oriented toward the application and performance of logistics in the military field. This is evident in organizations such as the Army, where logistics is seen as the planning and execution of movement and support for forces. It encompasses both military art and science, knowing when and how to accept risk, prioritizing requirements, and balancing limited resources. All these elements require military art, while understanding equipment capabilities incorporates military science (EJC, 2016, p. 8).

It should be emphasized that military logistics has been broadly defined and constitutes all the operational structural support necessary to enable what may be possible in the strategic and tactical planning of military operations. This leads to the consideration that almost everything is feasible to develop in the field of military tactics, but only logistics significantly makes it possible and determines how far it can go. The current nature of military logistics management and the support it provides accumulates responsibilities based on the planning and conduct of sustainment operations that involve production, reverse logistics, acquisition, general support of engineers, storage, field services, transportation, delivery, and maintenance (EJC, 2018, p. 28).

This indicates that this broad spectrum of integration of functions and responsibilities aims to meet complex needs, where logistics is responsible for obtaining and managing flows of sensitive information that require maximum security for both itself and its processes and procedures. The information and the management of its infrastructure carry critical weight that must be considered. Therefore, knowledge of this information gives rise to protection under cybersecurity, given the advantageous conditions that must be highlighted, in light of the threats and capabilities that they represent or knowledge arising from their operation, or the so-called integrated logistics management system, a term used within the Army, on which the cross-cutting flows of the exercise are specified.

Cybersecurity and Supply Chain

Following the structure of this document, it is established that cyberspace, recognized as the fifth domain of security, exists. This category has necessitated ensuring its safety, an intention fueled by various forms of the emergence of cyberspace itself. Furthermore, it has been reinforced as a concept of power and defense, contributing to the utilization of new technologies that unveil resources accessible to various actors within the international system as a tool for maintaining the balance of power. This practice is becoming increasingly essential in a world that is progressively digitalized and, therefore, more susceptible to cyberattacks, both internal and external. The significant benefits it offers make it an increasingly appealing pursuit for cybercriminal organizations (UNIR, 2022).

Thus, organizations of all types implement measures to confront and anticipate attacks, but above all, to strengthen detection and correction actions that build trust and facilitate the effective performance of the organization's activities. Similarly, creating a scenario informed by the military domain accounts for its cybersecurity relationship by addressing various risks and threats posed by adversaries of peace, regional stability, the proliferation of terrorism, and the diverse capacities to dismantle transnational criminal structures that seek to undermine states' military capabilities and strategic alliances. Given this context, the significant technological dependence of our society is a verifiable reality that is essential for the proper functioning of States, their security forces and agencies, and their infrastructures. This dependency is expected to increase in the future. Information technologies enable nearly everything our military forces require: logistical support, command and control of forces, real-time intelligence information, and much more (Díaz del Río Durán, 2011, p. 220).

Cyberspace must be considered a dimension to which conflicts and wars are transferred, restricting the limits of action of threats. This requires the full attention of military strategists, which can be decisive in the intention to subdue the opponent or enemy. Otherwise, neglecting the use of cyberspace against the actions of the defense and security forces of states can pose a significant self-constructed threat due to the low costs required to cause damage through the employment of skilled programmers capable of finding the most sensitive vulnerabilities in all defense systems, weapons, and, above all, the systems deployed for logistical support. These vulnerabilities can reveal strategic logistical locations and information related to the provision of sustainment training and its methods.

In his compilation of elements and introductory events regarding a study as a state-of-the-art on cybersecurity, Joyanes Aguilar (2011) highlights the relationship between cybersecurity and the military sector. He mentions, among other aspects, that cyberspace and cyber defense constitute a battlefield, acting as a strategic national asset. This situation compels decision-makers to defend military networks, which encompass air, land, sea, space, and cyberspace domains in relation to warfare subordinate to national security (p. 31).

Similarly, an approach is taken to situations deemed catastrophic, resulting from a lack of strategies and a misunderstanding following cyberattacks related to military logistical and nuclear secrets. This includes access to military logistics information not initially classified, which reveals sensitive issues involving economic and acquisition systems. Consequently, this leads to the emergence of terms such as "cyber weapons," referring to equipment that complements conventional weapons typical of theaters of operations (p. 34) in efforts to control high-impact cyberattacks.

Cyber Defense and Supply Chain

As mentioned, the intention is to develop components that can alert and intervene for early and reactive detection of isolated intrusions into the reserved information flow networks, thereby preventing potential cyberattacks from organizations or foreign nations.

Thus, the concept of cyber defense is established as a measure against cyberattacks. In simple and practical terms, it corresponds to a reluctance to engage in deliberate actions that would cause harm or consequences to an adversary, aimed at obtaining favorable outcomes in military operations. According to IBM (n.d.), "A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device." Furthermore, in support of this, the Inter-American Defense Board, through Ganuza (2020), establishes that cyber defense is an organized and prepared capacity to combat in cyberspace, which includes defensive, offensive, and intelligence activities (p. 14). He regards military cyber defense as the unit that connects cyber defense to the military art of utilizing cyberspace and army operations in cyberspace (cyberoperations), proposing a taxonomy of the various types of cyberoperations (p. 8).

For the International Telecommunication Union (ITU), "cybersecurity is the collection of tools, policies, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the availability, integrity, and confidentiality of assets in the connected infrastructures" (ITU, 2021, p. 12).

The relationship between cyber defense and cybersecurity, particularly in the military field, must first be understood based on actions taken by state entities, guided by policies that interact in an organized manner to engage in cyberspace, involving both defensive and offensive operations within military intelligence. The second aspect is, consequently, the measures formulated and adopted by the operational and tactical military strategy, which are established to prevent or mitigate to the greatest extent possible the impacts on sensitive and non-sensitive information management systems that provide detailed insights into the military assets (equipment, infrastructure, personnel management, and capabilities) of a nation or state used for its defense and security. All of the above relates to the actions executed by military logistics to manage the resources required to advance any military plan or operation utilizing demonstrated military capacity.

Military Logistics, Cyber Defense, and Cybersecurity

In this regard, the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE, 2023) highlights the importance within the Alliance of

> cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea [...] to shed more light on the practical implications, broader deterrence and defence [....] integrat[ion] into operational planning and Alliance operations and missions [...,] more effective organisation of NATO's cyber defence and better management of resources, skills, and capabilities.

Therefore, such influential organizations recognize the threats present in cyberspace, taking into account the performance environment in military operations and how security impacts them, in addition to the significant challenge posed for the wide range of actors, interests, resources, and collaborative capabilities. In this context, utmost information security must be prioritized, focusing on the mission's success and exercising control to achieve the desired objectives.

Preparation in military cyber defense and cybersecurity requires decisions based on the precepts emerging from the concept of what national cyber defense should entail. Thus, it must be supported by other fields of State action, such as the economy and national logistics, to support military and sustainment logistics. This support serves first as a means of financing and second as part of the national mobilization strategy (integration of the fields of state power to confront a war) if required.

The previous discussion highlights the necessity of linking cyber defense and cybersecurity with military logistics, creating a union of conceptual, organizational, and exceptional efforts to enhance the performance of defense and security operations. In this manner, military cyber operations[1] aligned with the Army's mission must interconnect, focusing on generating effects that support the objectives of the sustainment logistics mission. Consequently, cyber operations are linked through a coordinating axis that encompasses the technical, logistical, and administrative capabilities essential for the redundant benefit of planning and conducting military operations, all based on the premise of bolstering the security of networks and support systems, fostering surprise and initiative, and obstructing the intentions of threats and enemies seeking to exploit knowledge of logistical advantages and their support.

The relationship between military logistics and cybersecurity is based on the following conditions: military logistics encompasses techniques that frame the planning, implementation, and monitoring of various supplies and equipment, along with physical and financial resources, as well as personnel specialized in satisfying essential elements and supporting the needs of military operations. This discipline is thus regarded as the primary link that ensures the optimal performance and fluidity of critical and standard equipment, its supplies, and the highest degree of availability at the right time and place. Currently, in the information age, military logistics is also impacted by cyberattacks, which are influenced by information and communication technologies (ICT) that enable the management and coordination of its appropriate means, highlighting the importance of protecting it from vulnerabilities to cyberattacks, theft, or the compromise of its information.

The above entails dangerous effects for the development of military operations, since cyberattacks aimed at logistics information networks and, in general, all their systems could hinder or render useless the flow of information and goods, along with their respective elements: services, supplies, maintenance, and unique operations. This would imply a decrease in operational certainty, as well as the readiness and effective response capacity required by operational military tactics.

So, adopting cybersecurity measures for the Army's logistics chain systems and supply chain involves designing strategies to preserve the information and communication systems used in integrated military logistics management systems. This must include risk identification, designed channels, verification protocols, and training of exceptional talent in logistics to enhance improvement and resilience against potential cyber threats.

1 Cyber operations are military operations that take place in cyberspace with the same objectives as those of the classic dimensions of the theater of operations: to hold the lead over, preserve it, place the enemy at a disadvantage, and exploit it (Real Instituto Elcano, 2014).

In summary, military logistics and cybersecurity are interrelated due to their increasing reliance on information and communication systems, as well as their significance in military operations. Furthermore, without comprehensive logistics systems to support operations, the chances of success and mission fulfillment will be deemed low.

Design of the Supply Chain of the Colombian National Army

It is necessary to outline how the Army's supply chain is designed in order to distinguish its operation and present its participants, flows, and support for resource relations, planning, procurement, logistics management, and the maximum distribution channel. This chain is defined as the interaction of three processes that comprise the Force's logistics management macroprocess: logistics planning, acquisition of goods and services, and logistics operation (EJC, 2023).

Table 1. *Design of the Supply Chain of the Colombian National Army*

<table>
<tr><th>Process</th><th>Function</th><th>Objectives</th><th>Process management</th></tr>
<tr><td>Logistics planning</td><td>Lead logistics through the creation of strategies and their alignment in the organization</td><td>To control and measure logistics management, production, supply, maintenance, technical services, and transportation</td><td rowspan="2">Storage
Audit and inventory reconciliation
Hiring of units, budget executors, and administrative centers
Quality control of quartermaster products
Design, research, and development of quartermaster products
Delivery
Export
Maintenance of production machinery.
Third-level maintenance of weapons. Third-level maintenance of armored helmets
Second-level maintenance of tactical and optronic vehicles and weapons, mobile maintenance units
Third-level maintenance of optronic vehicles
Third-level maintenance of tactical vehicles
Customs clearance
Production planning
Quartermaster material production
Reception
Registration and registration certificate of aircraft
Functional rehabilitation
Processing of LOAs and amendments
Transport</td></tr>
<tr><td>Acquisition of goods and services</td><td>Identify needs, select purchase mode, and administer the useful life of the good or service for the sustainability of the Army</td><td>To acquire goods and services required by the Force through processes, following good logistics practices that satisfy the needs and achieve the sustenance, projection, and timely support of the Force</td></tr>
</table>

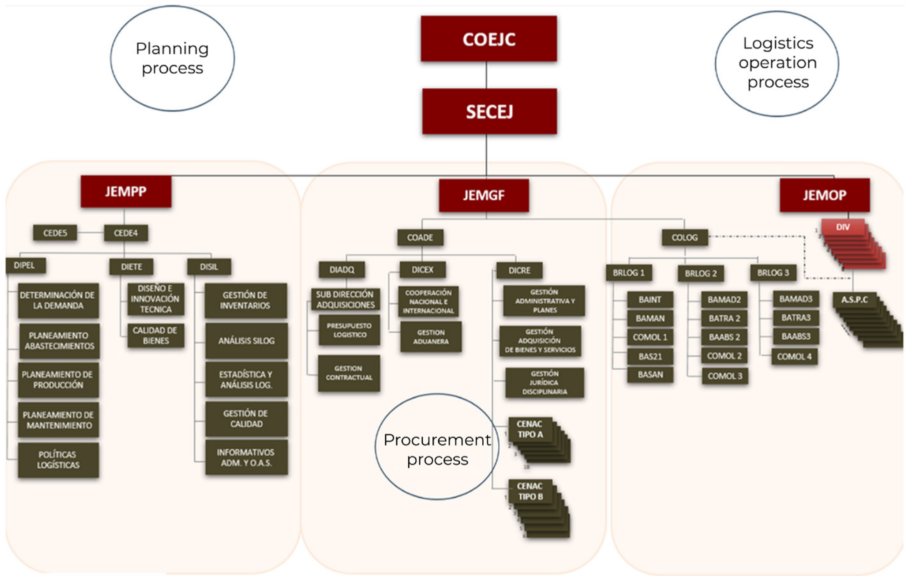
Logistics operation	Part of the supply chain that consists of calculating, preparing, arranging, organizing, delivering, and monitoring materials, goods, and services from the point of origin to the point of consumption, and meeting the needs for the functioning of an Army and its operations	To guarantee the optimization of the supply chain in the quantities, place, time, and conditions required by the men and units of the Army to sustain military operations and the functional rehabilitation of personnel injured in combat	Procurement Maintenance Production Reverse logistics Engineers for general support Storage Campaign services Transport Delivery

* According to the processes, functions, and objectives of the Army's integrated logistics management system.

****LOA:** Letter of Offer and Acceptance.

Source: Sistema Integrado de Gestión Logística del EJC (2023).

Figure 2. *Integrated Logistics Management System, Army's Supply Chain, and Its Processes*



Source: Own elaboration based on Sistema Integrado de Gestión Logística del EJC (2023).

Figure 2 shows the processes, functions, and objectives seen from the organization and its managers, graphically establishing its three essential moments: planning, procurement, and implementation of military logistics and sustainment itself. Its structural design gives rise to formalizing the conceptual similarity established from the difference between the supply chain and the logistics chain.

Table 2. *Differences between Supply Chain and Logistics Chain*

	Supply chain	**Logistics chain**
Scope	Covers all activities involved in the production, management, and distribution of goods and services	Focuses specifically on the movement and storage of goods
Objectives	To ensure that the right products are available at the right time and place	To ensure the timely and efficient delivery of goods and services to customers
Activities	Supply, manufacturing, and distribution	Transport, storage, and order management

Source: ISIL (2023).

Complementing the meaning of the sustainment WFF in logistics operations, production prioritizes the supply chain over the logistics chain. Therefore, it is important to highlight the influence of technological support that enables effective control over the supply chain and its management of logistics information in the Army, which entails managing not only information but also resources, means, and goods. The Ministry of National Defense (MDN, 2023) defines the Logistics Information System (SILOG, by its Spanish acronym) as:

> an integrated computer system that unifies all functions of organizational administration in real time and works on the integration of the logistics departments of all Forces to optimize goods and resources, enhancing the supply of troops, maintenance of equipment, and procurement of supplies. It is an ERP-type information system where all logistical and financial processes are managed on the same platform, becoming an indispensable support tool for planning, control, and supervision within the sector. (para. 1)

In terms of its function, the SILOG

> develops, integrates, and implements the administrative, logistical, and financial processes of the Defense sector within an integrated information system, using best practices and modern technology for optimal control and administration of resources designed to effectively support the operations carried out by security forces. (para. 3)

Table 3. *SILOG Logistics Information Management*

Logistics Module	Maintenance Module	Financial Module
All the logistical processes of the Military Forces must be uploaded to the SAP platform to control and verify each step, from procurement until the arrival of elements to the end customer.	Procedures are set for improving and maintaining the aircraft of the security force and light weapons.	Financial management of the movement in the Logistics and Maintenance Modules. Financial information entered into the system is processed, and compliance with accounting and tax regulations is evaluated.
• Purchasing • Inventory management • Production • Sales • Acquisition plan • Quality	• Aeronautical • Naval • Land • Biomedical • Weapons • Communications • Human resources	• Fixed assets • Accounting • Budget • Costs • Treasury
Technical Module Its purpose is to provide technological guidance, maintain applications, and guarantee the security and availability of the platform on which the information system operates. **Security and Access Control Module** Its purpose is to manage the users of the Logistics Information System, guaranteeing the confidentiality of the information and allowing access only to authorized personnel. **Training for Work Module** Its purpose is to facilitate the organizational change involved in implementing the SAP system in the security force. It has three lines: In-person Training, Blended Training, and Awareness Raising.		

Source: Own elaboration based on MDN (2023).

Table 3 illustrates the quality and magnitude of the information accumulated on the SAP platform, which is essential for managing goods, resources, and warehouse stock represented by various types of supplies. This includes information that reflects the capacity dimensions in several areas, existing as sensitive data within the supply chain of the entire defense sector organization, including the Military Forces and the Colombian National Army. Additionally, from the Army's logistics infrastructure and its tactical and technical units responsible for logistical operations, the information is enhanced, indicating that the Force currently has 46 Combat Service Support units (battalions) with individual capabilities that align regionally with the distribution of territories among divisions, brigades, and other joint commands. This constitutes a broad network that connects the capabilities vital for the planning phases of offensive, defensive, and defense support of civil authority military operations.

This organization also requires that there be information management at its level concerning administrative aspects that involve transportation equipment, fuel quantities and consumption, equipment maintenance systems, outstanding personnel in logistics, storage and inventory management tasks, health and communications support elements, along with distribution, delivery, and supply capabilities in each area of responsibility. Therefore, once the relationship among military logistics, cybersecurity, and cyber defense is established and formalized, it creates an information management link that merits closer examination and greater interest from academia and its generation of doctrine aimed at protecting the security of this valuable information.

Cyberattacks on the Army's Supply Chain

Comprehensive logistics[2] and cyberspace[3] can be seen as power factors and efficiency multipliers in maintaining military logistics in various ways, which serve as the foundation for the breadth of academia and doctrine aimed at promoting the study of cybersecurity in military logistics and its information management and flow systems:

Security and Optimal Resource Management

Military logistics involves effectively managing resources to acquire means, supplies, maintain equipment, and prepare personnel. The cybernetic systems and tools used to fulfill these functions facilitate real-time monitoring and tracking of such resources. The proper operation of logistics systems allows for decision-making based on demand forecasts tailored to the military logistics system, enhancing resource management and administration. Additionally, cyber systems help identify and prevent logistical problems, such as inaccuracies in supplies or equipment maintenance, thereby improving resource utilization.

About the defense sector in Colombia, it is essential to highlight the importance attached to this aspect by adopting the sector strategy established as a methodological guide for planning by capabilities (MDN, 2018) in response to ensuring that the Force structure fulfills its constitutional mission of providing

2 New organization and management model through which all processes and departments are coordinated to redirect efforts in the same direction (Esnova, n.d.).

3 Boundless non-physical world where any person can be interconnected over the internet, in such a way that they can interact with the entire world without barriers.

security and defense. The projection and development of the Force structure seek to guarantee that security forces are sustainable and efficient in the present and future (p. 4).

However, entities or organizations such as the National Army and, generally, the Military Forces can be the focus of attacks on their supply chains using various channels. Such is the case of using information from external providers, which is vulnerable to attacks on their information. In the face of events like this, there are three primary attacks or classes of events: 1) physical supply chain threats, which usually require cooperation with manufacturers and vendors; 2) digital supply chain threats: To decrease development time, software developers use a common third-party library to run a function in their applications on information and access to digital tools, and 3) business email compromise to trick recipients into providing sensitive data or sending money (Proofpoint, 2023, para. 7).

Examples of the above include the attack on the Supply Chain Management System in 2018 and an extensive cyberattack targeting the supply chain management system of the U.S. Department of Defense, known as the SolarWinds cyberattack. This complicated the security of data related to suppliers and their logistical connections, endangering the supply chains of the Military Forces (BBC News Mundo, 2020, para. 1).

Automation as a Security Factor of the Logistics Management System

Advances in cyber technologies and automation techniques streamline and optimize military sustainment logistics operations. They perform administrative tasks efficiently, freeing up human personnel and achieving exceptional performance alongside more complex management. An example is the use of military satellites to enhance the efficiency of supply chain operations. Military satellites provide a platform for further automating logistics and supply chain management. By utilizing artificial intelligence, military satellites enable automated data analysis, allowing supply chain managers to make better decisions in a fraction of the time. They are revolutionizing supply chain logistics and management, enhancing communication, asset tracking, and automation by facilitating improved decision-making (Frąckiewicz, 2023).

The above outlines the future direction of development based on the use of technologies that support supply chains within military sustainment logistics. Although it requires resource allocation, it highlights strengths that deserve greater attention from academia in strengthening the connection among cybersecurity, cyber defense, and military logistics. The more advanced and technologically supported military logistics are, the greater the dependency, thus necessitating increased focus on cybersecurity to enhance the security of military logistics systems.

Logistics Communication and Coordination Systems

Military logistics requires tools that, in many notable cases, provide rapid communication between structures and command levels. Logistics systems supported by information technologies must ensure decision-making through secure channels, achieving effectiveness and maximum situational accuracy regarding materials and supplies of the supply chain of the military logistics management system, thereby enhancing the speed of the logistics response for sustaining military operations.

The supply chain has not been alien to the impact of technologies that positively influence its operation. This contribution is also formalized in the administration of military logistics, always to analyze timely and detailed information based on the quality of logistical support, influencing issues such as cost reduction, reduction of waiting times, and improving administration in supply flows of various kinds. Simchi-Levi et al. (2000) list the goals of technology in supply chain management:

> 1) collect information on each product from production to delivery or purchase point, and provide complete visibility for all parties involved; 2) access any data in the system from a *single-point-of-contact;* 3) analyze, plan activities, and make trade-offs based on information from the entire supply chain. (p. 223)

The above emphasizes the importance of processes that account for the adaptive improvements achieved by implementing information management methods and models. These processes help demonstrate the formalization of potential deficiencies, as well as the threats or risks associated with managing this information, to enhance cyber defense in military logistics and strategic operations within its comprehensive operating system.

Security and Protection Strategies of the Integrated Military Logistics System

Cyberspace plays a crucial role in the security and protection of military logistics. Cybersecurity systems are able to detect and alert the military logistics system to cyberattacks, thus safeguarding the procedures and information deemed critical to military logistics. Collectively, cybersecurity methods enhance security within the supply chain, ensuring the legitimacy and authenticity of the goods and materials utilized for the operation of the logistics system and the Military Forces.

However, beyond the strategy to achieve military objectives, anticipation may be more important. Therefore, anticipating this particular case and properly addressing the threats directed at the logistics management system must be structured as an initial part of the strategy (advanced preparation). Based on this principle, Esbry (2021), recognizing the importance of the strategy and its applicability to safeguard logistics information, argues that the characteristics of contemporary conflicts confirm the relevance of the art of war as philosophical principles, which range from strategic to tactical and also encompass areas essential to the conduct of war such as economics, education, politics, diplomacy, industry, etc. (p. 42).

The above invokes what was considered in the work of Sun Tzu, who appreciated the importance of living in a qualified manner within his philosophical current focus on "winning the war sooner." In this way, it is essential that the Army studies and properly yields results from this correlation to perfect its structures and logistical support operations, preserving its operational capacity in the face of any possible threat and scenario, especially those related to cyberattacks and those aimed at weakening the operational support logistics apparatus.

Having said that, several theories, hypotheses, and management practices create a framework for analyzing military logistics, today's sustainment WFF, and the relationship with cybersecurity, which could serve as a foundation for developing literature and doctrine in military logistics.

Theory of Dual-Use Goods and Technology[4]

This theory maintains that technology and systems developed in civilian sectors can be used for military purposes. In this context, supply chain management techniques employed in the commercial sector and the associated technology can likewise be applied to achieve military objectives. This reality highlights the increasing urgency of protecting these systems against potential cyber threats.

In this regard, the methods used in supply chain management, both commercially and technologically, can also serve military objectives and

[4] Product or service that can be used for both civil and military purposes, that is to say, the product or service is generally intended for civil use, for example, in industry, but which can also be used to develop weapons or military material, or vice versa (Francia diplomacia, 2014).

achievements, which heightens the need to protect these systems from potential cyber threats. This relationship is further articulated in Buzan's conception (1998). He argues that the aspects impacted by this technological revolution are closely related to advancements in the civil sector. The application of dual-use techniques in communications, mobile phones, and intelligence underscores the unified nature of the Industrial Revolution. Therefore, every industrialized society maintains a military capability, thanks to the knowledge, material, human, and financial resources developed. This presents a challenge in separating the civil applications of technology from its military uses (p. 156).

Shared Risk in Cybersecurity[5]

This practice indicates that business and military entities, along with their suppliers, are at risk of a potential cyberattack. In this context, companies providing military logistics services or facilitating their provision are expected to take responsibility for the cybersecurity of their internal techniques and procedures to prevent possible harmful impacts on the Force's capacity, which could affect their design approach for employment in defense provision.

This aspect is exemplified in two ways. One way is the orientation of the employment of armies and how they contribute to their cyber defense, assuming positions of technological support, as well as their importance in supply chains and their respective value within military strategy. The other way is the position of the companies that provide technology, not only computer technology, but also the industry that offers weapons systems and critical-use equipment. Additionally, we have the position of Fernández-Montesinos (2016), who discusses how everyday technology transforms war and the actions of armies and their logistics. War is a logic of transformation that can sometimes reverse the situation, turning what was a strength into a weakness. This increase is due to failures, breakdowns, and vulnerabilities, which also require a complex logistics chain (p. 8).

The second way or position is identified in Seguridad en América (2021), which proposes not only commenting on the importance of cybersecurity but also argues for moving from theory to action. For this media outlet, in the dynamism and digitalization that we live in, we cannot ignore where trends are leading us; within the security framework, we must always balance people, processes/procedures (under legal framework), and technology, which increasingly plays more significant roles on a day-to-day basis, supporting us in enhancing our operational efficiency (para. 7).

5 What companies need is a new way of looking at risk and a more collaborative manner of identifying and addressing the risks they face (PWC, 2024).

The above must encompass everything from the political actions and positions of the States to the slightest interventions by actors, including the responsibility of those who manage the security of military information and the protections that must be implemented in the army's supply chains.

Control Theory[6]

This theory maintains that, in a military environment, extensive control over the entire supply chain and its related systems is necessary. This restricts the proportion of cybersecurity measures in undivided aspects of the same supply chain, starting from the acquisition of raw materials, services, and goods intended for production and subsequently moved to storage until they are involved in processes or operations that sustain delivery in areas of need or combat. The entity's own missionary and operational activities must be managed alongside controls that help protect its most valuable asset: information. An organization aiming to be increasingly competitive must prioritize information protection, avoiding exposure to malicious individuals or potential cyberattacks (MangeEngine, 2022, para. 1).

Theory of Resilience or Cyber Resilience[7]

It focuses on an organization's ability to recover quickly from a cyberattack. In this context, military logistics companies must implement cybersecurity measures to minimize the risks of a potential attack and ensure rapid recovery should an incident occur. According to SAP (2020), we have been globally affected by an unprecedented event, which we did not anticipate and which we had very little time to maneuver to stay safe, adapt ways of working, and readjust our consumption habits. Faced with this panorama, many companies must ask themselves, What is my recovery capacity and time so that my logistics operation can be reestablished in the event of an emergency? The answer is resilience. Any supply chain must have this concept in its DNA to get ahead of the contingency (para. 1-2).

In summary, these theories, hypotheses, and management practices highlight the importance of cybersecurity in the Army's military logistics chain, supply chain, and integrated logistics management system, as well as the necessity to implement

[6] Control theory deals with the "control system" of "dynamic systems" in engineering processes and machines. The goal is to develop a model or algorithm that governs the application of system inputs to drive it to a desired state, minimizing any delay, overshoot, or steady-state error (William, 1996).

[7] Cyber resilience describes the ability of a system or organization to resist or recover from cyberattacks or incidents. A cyber-resilient organization works to protect its digital assets and the continuity of its systems against cyberattacks or technological disasters (S2 Grupo, 2023).

measures to protect these systems from potential vulnerabilities, which could lead to considerable consequences resulting in the deterioration of military operations. Therefore, based on this accumulation of concepts, the documentary management of doctrine formation is established, which involves designing a greater number of reference, campaign, and technique and procedure manuals that influence the performance of tactics aimed at protecting supply chains in the Army.

SWOT Matrix. Cyber Defense of the Army's Supply Chain

Table 3 presents the SWOT matrix that analyzes the importance of increasing the study of cybersecurity in military logistics.

Table 4. *SWOT Matrix*

SWOT ANALYSIS	**STRENGTHS** • Greater security in the management of military information and data • Reduction in the risk of cyberattacks and vulnerabilities in the supply chain • Commitment to modernization and continuous improvement of military capabilities	**WEAKNESSES** • Budget limitations for the implementation of large-scale cybersecurity measures. • Lack of trained personnel and technological resources to implement cybersecurity measures • Resistance to change by some personnel or suppliers unfamiliar with cybersecurity measures in military logistics
OPPORTUNITIES • Improve supply chain efficiency by implementing cybersecurity measures. • Increase the response capacity to possible cyberattacks, thereby improving resilience • Potentially reduce costs related to recovery from cyberattacks thanks to prevention	**SO STRATEGIES** 1. Use of resources: Use the information, resource, and asset management platforms of the integrated logistics management system and set guidelines for innovation and process adjustment 2. Strategic alliances: Establish alliances with other organizations in academia and business, leading to increased measures that support cybersecurity in the supply chain 3. Diversification: Use internal strengths to diversify measures by involving the largest number of participants in the supply chain, from suppliers to those responsible for managing resources of any kind 4. Geographic expansion: Use internal strengths to expand cyberattack management experience, find expert personnel, and disseminate criteria, procedures, and strategies. Promote the formation of interdisciplinary teams to open the door to research and doctrine based on the collection of information	**WO STRATEGIES** 1. Develop strategic alliances: Use external opportunities to develop alliances with other companies or sectors that can help overcome internal weaknesses 2. Improve the training and development of human talent that manages the supply chain through improved guidelines for personnel training and development, overcoming the deficiency and lack of specific technical skills. Everything must be oriented from academia and doctrinal updating 3. Innovation and development of new products or services: Use external opportunities to promote innovation and the development of new programs and studies that allow updating doctrine and increasing academic development to avoid cyberattacks on the Army's logistics supply chain 4. Improve internal processes: Take advantage of external opportunities to improve the internal processes of the Army's logistics, overcome weaknesses, and improve the efficiency of supply chain information management in the integrated logistics management system

THREATS	ST STRATEGY	WT STRATEGY
• Lack of political support or available resources for implementing cybersecurity measures • Increase in cyberattacks and cyber threats • Government or industry requirements that do not fit current technical capabilities	1. Improve quality and efficiency: Use internal strengths to improve the quality and efficiency of production processes and logistics operations that exhibit vulnerabilities in managing supply chain information 2. Develop new skills and competencies: Use internal strengths to develop new skills and competencies to confront threats 3. Search for new academic spaces in education and training centers and structures 4. Establish strategic alliances: Use internal strengths to establish partnerships with other Forces by sharing experiences with the supply chains that make up the logistics chain of the Military Forces	1. Increase the competitiveness of the Force, its integrated logistics management system, and its supply chain via strategic proposals taken to political actors seeking to strengthen support against cyberattacks on military logistics 2. Increase the capacity to adapt by developing new digital skills based on research to face the growing proliferation of threats 3. Use academia, research, and innovation from the formation of interdisciplinary groups that contribute and promote the resources allocated to increase the doctrinal proposals in handling cyberattacks on the Army's supply chain

Source: Own elaboration.

In general, the results of the SWOT matrix suggest essential benefits to increasing the study of cybersecurity in military logistics, such as enhancing the efficiency of the supply chain and improving the ability to respond to potential cyberattacks. However, obstacles such as financial constraints and the need for more trained personnel and technological resources may arise. By addressing these challenges, the Army can improve its operational capabilities and readiness to confront both traditional and emerging threats to the Force's logistics chain, supply chain, and integrated logistics management system in the sustainment WFF.

Conclusions

Cybersecurity and cyber defense are fundamental components that ensure the integrity and confidentiality of the Army's logistics chain and, consequently, its integrated logistics management system. Conducting studies on cybersecurity, cyber defense, and military logistics will enhance the institution's capabilities to protect and secure information systems and networks related to the acquisition system, administrative management, stock management, equipment maintenance, system capabilities, and the sustainment WFF operationalized in its units and methods.

Cybersecurity and cyber defense are crucial to avoiding cyberattacks that could cause significant damage to infrastructure, military operations, and national security by obtaining information that allows the Army to establish its operating capabilities.

It is essential that academia, structured by the organizations in charge of doctrine and the educational system of the force responsible for training and managing logistics and sustainment resources, provide an overview of the impact needs on which the constructs are built to enhance specialized and advanced knowledge in cybersecurity and cyber defense, aimed at strengthening military logistics applied to the Army and training highly qualified and comprehensive professionals in these areas.

The integration of cybersecurity and cyber defense in military logistics and doctrine will improve resource management and decision-making, resulting in greater operational and logistical efficiency.

The limited research on cybersecurity, cyber defense, military logistics, and the Army's integrated logistics management system hinders the creation of effective strategies and tactics to address cyber challenges and threats within the Force's supply chain.

Training in cybersecurity and cyber defense within the military academy provides the skills and knowledge necessary to prevent and mitigate cyber risks in its supply chain environment; hence, the importance of academia's intervention in the face of this challenge.

A course that includes cybersecurity, cyber defense, and military logistics, along with their respective supply chains, will foster strong collaboration and support among similar parties involved in safeguarding military systems.

The advancement of this knowledge will facilitate the adaptation and modernization of the tactics and methodologies used in cybersecurity and cyber defense to face the events, threats, and vulnerabilities that arise regularly.

The importance of academia conducting these studies lies in the necessity to train competent military leaders who can make informed and valuable decisions in cybersecurity and cyber defense to protect national interests and ensure the security of the supply chain for the integrated logistics management system of the Colombian National Army.

References

Buzan, B. (1998). Introducción a los estudios estratégicos: Tecnología militar y relaciones internacionales. *Cuadernos de Estrategia*, (99), 155-1166. https://dialnet.unirioja.es/servlet/articulo?codigo=4553585

Centro de Doctrina Conjunta [CEDOC] (Ed). (2018). *Manual Fundamental Conjunto MFC 1.0 Doctrina Conjunta.* Sello Editorial ESDEG. https://doi.org/10.25062/MFC10

Corera, G. (2020, December 20). SolarWinds: 5 ataques informáticos de Rusia que transformaron la ciberseguridad en Estados Unidos. https://www.bbc.com/mundo/noticias-internacional-55381892

Council of Supply Chain Management Professionals [CSCMP]. (2023, October 20). Council of Supply Chain Management Professionals. https://cscmp.org/

Díaz del Río Durán, J. (2011). La ciberseguridad en el ámbito militar. *Cuadernos de Estrategia*, (149), 215-256. https://dialnet.unirioja.es/servlet/articulo?codigo=3837348

Ejército Nacional de Colombia. (2016). *MFRE 4-0 Sostenimiento.* Imprenta Ejército. https://www.cedoe.mil.co/enio/recurso_user/doc_contenido_pagina_web/800130633_4/458784/mfre_4_0_sostenimiento.pdf

Ejército Nacional de Colombia. (2018). *Manual de campaña.* Imprenta Ejército.

Ejército Nacional de Colombia. (2023, January 3). Sistema Integrado de Gestión Logística. https://www.ejercito.mil.co/sistema-integrado-de-gestion-logistica/

Esbry, G. (2021). Pensamiento estratégico de Sun Tzu: Su legado a través de la historia. *Revista Visión Conjunta*, (25), 39-42. http://www.cefadigital.edu.ar/bitstream/1847939/2013/1/ESGCFFAA-revista%20Visi%C3%B3n%20Conjunta-25.pdf

Fernández-Montesinos, F. (2016, November 30). Los militares y la tecnología [Documento de análisis, n.º, 72]. https://www.ieee.es/Galerias/fichero/docs_analisis/2016/DIEEEA72-2016_Militares_Tecnologia_FAFM.pdf

Frąckiewicz, M. (2023). El impacto de los satélites militares en la logística militar y las cadenas de suministro. https://ts2.space/es/el-impacto-de-los-satelites-militares-en-la-logistica-militar-y-las-cadenas-de-suministro/

Fuerza Aérea Colombiana [FAC]. (2016). *Manual de doctrina logística -MALOG-*. Imprenta y Publicaciones Fuerzas Militares República de Colombia. https://www.fac.mil.co/sites/default/files/linktransparencia/Planeacion/Manuales/manuales2022/malog_2016.pdf

Fundación Universitaria Internacional de la Rioja [UNIR]. (2022). ¿Qué es la ciberseguridad? Objetivos e importancia en la actualidad. https://colombia.unir.net/actualidad-unir/que-es-ciberseguridad/#:~:text=La%20ciberseguridad%20o%20seguridad%20inform%C3%A1tica,programas%2C%20de%20posibles%20ataques%20digitales.

Ganuza, N. (2020). *Guía de ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.* Junta Interamericana de Defensa. https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6th ed.). McGraw-Hill. https://academia.utp.edu.co/grupobasicoclinicayaplicadas/files/2013/06/Metodolog%C3%ADa-de-la-Investigaci%C3%B3n.pdf

Hitzler, R., & Honer, A. (2016). Los métodos cualitativos. In H. Sánchez (ed.), *Análisis para el estudio y la enseñanza de la ciência política: La metodologia de la ciencia política* (pp. 59-68). Universidad Nacional Autónoma de México. https://archivos.juridicas.unam.mx/www/bjv/libros/13/6180/6.pdf

IBM. (n.d.). What is a cyberattack? https://www.ibm.com/think/topics/cyber-attack

International Telecommunication Union (ITU). (2021). *Guide to Developing a National Cybersecurity Strategy* (2nd ed.). https://ncsguide.org/wp-content/uploads/2024/05/508938E.pdf

ISIL. (2023). Diferencias entre la cadena de suministro y la de abastecimiento. https://isil.pe/blog/logistica/diferencias-suministro-abastecimiento/#:~:text=Actividades%3A%20la%20cadena%20de%20suministro,y%20la%20gesti%C3%B3n%20de%20pedidos.

Jiménez Jiménez, I. (2021). Elementos que identifican los métodos comparados. *Collectivus, Revista de Ciencias Sociales, 8*(2), 167-192. https://doi.org/10.15648/Collectivus.vol8num2.2021.3134

Joyanes Aguilar, L. (2010). Introducción: Estado del arte de la ciberseguridad. In Ministerio de Defensa (Ed.), *Ciberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio* (pp. 13-46). Imprenta del Ministerio de Defensa de España. https://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Lifeder. (2020). Investigación bibliográfica: Definición, tipos, técnicas. https://www.lifeder.com/investigacion-bibliografica/#:~:text=La%20investigaci%C3%B3n%20bibliogr%C3%A1fica%20o%20documental,selecci%C3%B3n%20de%20fuentes%20de%20informaci%C3%B3n

MangeEngine. (2022, July 21). ¿En qué consiste un control en ciberseguridad? https://blogs.manageengine.com/espanol/2022/07/21/que-es-control-en-ciberseguridad.html

Martínez Corona, J. I., Palacios Almón, G. E., & Oliva Garza, D. B. (2023). *Guía para la revisión y el análisis documental: propuesta desde el enfoque investigativo.* Ra Ximhai: Revista Científica de Sociedad, Cultura y Desarrollo Sostenible, *19*(1), 67-83. https://dialnet.unirioja.es/servlet/articulo?codigo=8851658

Ministerio de Defensa Nacional [Mindefensa]. (2018). *Guía metodológica de planeamiento por capacidades.* http://capacitas.mindefensa.gov.co/storage/biblioteca/Guia_Metodologica_de_Planeacion_por_Capacidades.pdf

Ministerio de Defensa Nacional [Mindefensa]. (2023). *Sistema de Información Logística SILOG.* https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido?NavigationTarget=navurl://9f049c2f279e9248da04add30057f515

Montanyá, O. (2021, January 4). La logística: de la guerra al arte. https://micromegas.bsm.upf.edu/2021/01/04/la-logistica-de-la-guerra-al-arte/

NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2023, October 19). *NATO recognises cyberspace as a 'Domain of Operations' at Warsaw summit.* https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Organización del Tratado del Atlántico Norte [OTAN]. (2020). *Allied Joint doctrine for cyberspace operations.* NATO Standardization Office. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Parlamento Europeo, & Consejo de la Unión Europea. (2019). *Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo* de 17 de abril de 2019. relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=FR

Ponce Talacon, H. (2007). La matriz FODA: Alternativa de diagnóstico y determinación de estrategias de intervención en diversas organizaciones. E*nseñanza e Investigación en Psicología, 12*(1), 113-130. https://www.redalyc.org/pdf/292/29212108.pdf

Proofpoint. (2023). What Is a Supply Chain Attack? https://www.proofpoint.com/us/threat-reference/supply-chain-attack

Rodríguez Gómez, D. (n.d.). Elección de la metodología de investigación. In *El proyecto de investigación* (pp. 33-35). Universitat Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/147625/3/ElProyectoDeInvestigacion.pdf

Rodríguez Jiménez, A., & Pérez Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Escuela de Administración de Negocios,* (82), 175-195. https://journal.universidadean.edu.co/index.php/Revista/article/view/1647

Sánchez Acevedo, M. E. (2020). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. In E. S. Guerra & G. E. Medina-Ochoa (Eds.), *La seguridad en el ciberespacio: Un desafío para Colombia* (pp. 34-38). Editorial ESDEG. https://doi.org/10.25062/9789584288929.01

SAP. (2020, April 6). Construyendo la cadena de suministro resiliente en tiempos de contingencia. https://news.sap.com/latinamerica/2020/04/construyendo-la-cadena-de-suministro-resiliente-en-tiempos-de-contingencia/

Simchi-Levi, D., Kaminsky, P., & Simchi-Levi, E. (2000). *Designing and Managing the Supply Chain: Concepts, Strategies, and Case Studies.* McGraw-Hill.

Seguridad en América. (2021, June 13). *Ciberseguridad, menos teoría y más acción.* https://www.seguridadenamerica.com.mx/noticias/articulos/27840/ciberseguridad-menos-teorIa-y-mAs-acciOn