

A black and white photograph of a person from behind, wearing a headset, sitting in a control room. The person is looking at several computer monitors displaying data and charts. The background is a blurred cityscape at night with bokeh lights.

Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace

Milena Elizabeth Realpe Díaz
Angélica María González González
(Editors)

Cybersecurity and Cyber Defense Collection

Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace



Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace

MILENA ELIZABETH REALPE DÍAZ
ANGÉLICA MARÍA GONZÁLEZ GONZÁLEZ
(EDITORS)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., 2025

Cataloging in publication – Escuela Superior de Guerra "General Rafael Reyes Prieto"

Disruptive Technologies, Logistics, And National Security And Defense In Cyberspace / Milena Elizabeth Realpe Díaz and Angélica María González González, editors – Bogotá : Sello Editorial ESDEG, 2025.

152 pages : illustration and graphics; 24 cm
Includes bibliographic references at the end of each chapter

ISBN (print) : 978-628-7818-05-7
E- ISBN: 978-628-7818-06-4

(Cybersecurity and Cyber Defense Collection)

1. Disruptive technologies – National Security. 2. Cybersecurity – Military Defense. 3. Military Logistic – Technologic Innovations. 5. i. Galindo, Jaime Alonso, (preface) ii. Realpe Díaz, Milena Elizabeth (editor) iii. González González, Angélica María, (editor). iv. Giraldo Ríos, Lucas Adolfo (author) v. Ospina Navas, Jaider (author) vi. Barrios Torres, Sergio (author) vii. Maldonado, Carlos Eduardo (author) viii. Colombia. Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG).

SCLC QA76.9 A25 2025
SCDD 355.0335 2 23

Catalog Record SIBFuP 991360842407231



Downloadable file in MARC at: <https://tinyurl.com/esdeg991360842407231>

Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace

First edition, 2025

Editors:

Milena Elizabeth Realpe Díaz
Angélica María González González

2025 Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Office of the Deputy Director of Research
Sello Editorial ESDEG
Carrera 11 N°. 102-50 Bogotá D.C., Colombia
www.esdeglibros.edu.co

Cover:

Raquel Arianne Alvarado Candela based on images
from Adobe Stock

E-book published through the Open Monograph Press
platform.

Print run of 100 copies
Printed in Colombia

Cybersecurity and Cyber Defense Collection

Print ISBN: 978-628-7818-05-7

Digital ISBN: 978-628-7818-06-4

DOI: <https://doi.org/10.25062/9786287818064>

Translation of the book titled "Tecnologías disruptivas, logística, seguridad y defensa nacional en el ciberespacio", resulting from research conducted by the Escuela Superior de Guerra "General Rafael Reyes Prieto."

The content of this book reflects the authors' views and is their sole responsibility. The positions and statements presented herein are the result of an academic and research exercise that does not necessarily represent the official or institutional position of the participating institutions, the Escuela Superior de Guerra "General Rafael Reyes Prieto," the Military Forces of Colombia, and the Ministry of National Defense.



Books published by the Sello Editorial ESDEG are open access under a Creative Commons license: Attribution-NonCommercial-NoDerivatives 4.0 International.
<https://creativecommons.org/licenses/by-nc-nd/4.0/>



Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

Vice-Admiral
León Ernesto Espinosa Torres
DIRECTOR

Brigadier General
Nestor Favian Nieto Rivera
DEPUTY DIRECTOR

Colonel
Aldemar Serrano Cuervo
DEPUTY DIRECTOR OF RESEARCH



EDITORIAL ESDEG

Colonel
Aldemar Serrano Cuervo
HEAD OF SELLO EDITORIAL ESDEG

Erika Paola Ramírez Benítez
EDITOR IN CHIEF OF SELLO EDITORIAL ESDEG

Jorge Hernando Aristizábal Gáfaró
Felipe Solano Fitzgerald
PROOFREADERS

Raquel Arianne Alvarado Candela
LAYOUT DESIGNER

Nathalie Barrientos Preciado
TRANSLATOR

Table of Contents

Preface MG Jaime Alonso Galindo	09-10
Introduction Milena Elizabeth Realpe Díaz Angélica María González González	11-14
Chapter 1 Definition and Impact of Digital Transformation and Cibersecurity Lucas Adolfo Giraldo Ríos	15-42
Chapter 2 Blockchain and Cybersecurity: Building Digital Trust Jaider Ospina Navas	43-68
Chapter 3 The Colombian National Army's Logistics Chain, Cybersecurity and Cyber Defense: Attention to Academia Sergio Barrios Torres	69-98
Chapter 4 Cutting-Edge Sciences and Disruptive Technologies in Cyberspace as a Framework and Condition for Colombia's Cyber Defense Carlos Eduardo Maldonado	99-128
Chapter 5 Power in the Information Age: Perspectives on Cyber Power Milena Elizabeth Realpe Díaz	129-150

Preface

Major General Jaime Alonso Galindo

Former director, Escuela Superior de Guerra "General Rafael Reyes Prieto"

We live in an era marked by the accelerated evolution of disruptive technologies, a phenomenon that transcends traditional ways of understanding and addressing national security and defense in cyberspace. In this dynamic and challenging context, it is mandatory to conduct a continuous academic review of such dramatic changes to improve decision-making and the capabilities of organizations, public entities, and the Military Forces to face them most effectively.

This book aims to elucidate the unique characteristics of disruptive technologies, underscoring their transformative impact on national security and defense in cyberspace. As these innovations emerge and reshape our realities, their influence transcends technological realms, significantly altering national interests and the security of nations.

The work deeply analyzes current trends, unveiling the web of invisible but potentially catastrophic threats and attacks brewing on networks. Disruptive technologies swiftly supplant existing infrastructures, posing critical challenges to national cybersecurity and cyber defense. How do disruptive technologies and global logistics impact national security and defense in cyberspace?

In this intellectual journey, we will explore the essential distinction between cybersecurity and cyber defense, two pillars for addressing threats in cyberspace. Cybersecurity is the first line of defense, focused on protecting systems and data from cyber threats. However, to safeguard national integrity, we must go further, addressing cyber defense with strategies and policies that shield a nation against cyberattacks that could compromise its security and stability.

The prevailing need to analyze, prevent, and make prospective decisions in the face of disruptive technologies highlights the importance of the synergy between cybersecurity and cyber defense. In this context, this book presents

these crucial interrelationships, thus becoming an essential resource for those seeking to comprehend and confront emerging challenges in cyberspace.

Let us prepare to explore a field where innovation and security converge, and knowledge becomes the best tool against the invisible threats that lurk in the digital world.

Introduction

Milena Elizabeth Realpe Díaz
Angélica María González González
Escuela Superior de Guerra "General Rafael Reyes Prieto"

With the transition of the Industrial Age at the end of the 20th century and the emergence of the Information Age with the Fourth Industrial Revolution at the beginning of the 21st century, we have experienced a radical change regarding globalization. In this new paradigm, the internet has interconnected all individuals, making cyberspace a unique domain that challenges and redefines the traditional concepts of security and defense of States.

In contrast to conventional conflicts, characterized by specific regulations and doctrines, cyber conflicts and threats stemming from the cyber world, driven by the constant increase in digital density, give rise to a gray area marked by instability and uncertainty. This scenario is characterized by the absence of specific regulations and clearly defined conditions of action, which opens the doors to activities that are difficult to interpret and subject to existing rules.

The emergence of disruptive technologies, defined as "an innovation that helps create a new value network and eventually disrupts today's market (in a few years or decades), displacing a previous technology" (Dabirian & Loza Matovelle, 2015, p. 30), consolidates new stories through which society relates and develops.

This book, *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace*, is a comprehensive guide that examines, from various academic perspectives, the impact that disruptive technologies and logistics have on national security and defense. This examination is based on scientific and technological development, logistics, management, and digital security in order to understand changes in environments characterized by volatility, uncertainty, complexity, and ambiguity (VUCA) and facilitate more informed decision-making processes for national security and defense in cyberspace.

Chapter 1, "Definition and Impact of Digital Transformation on Cybersecurity," discusses strategic forecasting and foresight, where the former involves anticipating possible future scenarios and the latter seeks to identify emerging trends. It also highlights the need for strategies that promote cybersecurity awareness for a solid organizational culture in information security and concludes that by promoting such culture, organizational resilience to cyber threats is strengthened.

Chapter 2, "Blockchain and Cybersecurity: Building Digital Trust," explores the state of the art of this disruptive technology in order to identify its role in building a secure digital ecosystem. To do this, it specifies the features of blockchain, such as decentralization, immutability, and consensus, and discusses its advantages in terms of security, transparency, and resistance to manipulation. It also analyzes the types of immutability attacks known to date, describes the various applications where blockchain is used, and describes the current challenges and limitations, providing a holistic view of the possibilities and obstacles in this evolving field.

Chapter 3, "The Colombian National Army: Logistics Chain, Cybersecurity, and Cyber Defense," examines the strategic interest of the Force in studies on the relationship among cybersecurity, cyber defense, and military logistics. It emphasizes the need to expand knowledge in this area, both in academia and in updating military doctrine, to strengthen national security. Possible conceptual and action lags that could become operational weaknesses are listed, suggesting reflections as a basis for future research and doctrinal developments to improve and protect the military logistics chain of the Army from an emerging cybersecurity perspective.

Chapter 4, "Cutting-Edge Sciences and Disruptive Technologies in Cyberspace as a Framework of and Condition for the Cyber Defense of Colombia," problematizes the importance of complexity sciences, their foundations, themes, and problems amid the digitalization of the world and society concerning national security and defense. It upholds that complexity sciences are life sciences that deal with exactly everything that normal science ignores. Besides, there is an essential tension between science and technology: Science traditionally involves a principle of democracy, while the history of technology has always been that of *prima facie* military technologies. In brief, complexity sciences allow us to overcome or resolve this tension.

Finally, Chapter 5, "Power in the Information Age: Perspectives on Cyber Power," investigates the dynamics taking place in cyberspace, explaining how

cyber power is beginning to be talked about in the general sphere of power. For this, it examines the meanings of the term according to regional perspectives on the understanding that it is defined according to how it is grasped and where it is situated. The chapter also describes power from the perspective of the U.S. military and the European Union and expands the understanding of cyber power based on its location, all of which aim to establish adequate estimates of this subject matter.

We hope that this work will inspire the reader to analyze these new dynamics, thus contributing to the academic and technical discussion on cybersecurity and cyber defense.

References

Dabirian, R., & Loza Matovelle, D. (2015). Introducción a la tecnología disruptiva y su implementación en equipos científicos. *Revista Politécnica*, 36(3), 1-4. <https://n9.cl/su68o>

Chapter 1

Definition and Impact of Digital Transformation and Cybersecurity*

DOI: <https://doi.org/10.25062/9786287818064.01>

Lucas Adolfo Giraldo Ríos

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: This chapter discusses strategic forecasting and foresight. The former involves anticipating plausible future scenarios, while the latter identifies emerging trends. It highlights the need for strategies that promote cybersecurity awareness for a solid organizational culture in information security. It concludes that promoting this culture strengthens organizational resilience to cyber threats.

Keywords: cybersecurity; awareness raising; organizational culture; strategy; forecasting; foresight

* 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.

Lucas Adolfo Giraldo Ríos

PhD candidate in Engineering, Industry and Organizations, Universidad Nacional de Colombia. Master's in Technology-Based Business Management, Universidad Antonio de Nebrija, Spain. Master's in Innovation, Universidad EAN, Colombia. Specialization in Business Financial Management, Universidad de Medellín, Colombia. Bachelor's in Business Management, Universidad de Antioquia, Colombia.

<https://orcid.org/0000-0002-9947-7882> - Contacto: lucas.giraldo@esdeg.edu.co

APA Citation: Giraldo Ríos, L. A. (2025). Definition and Impact of Digital Transformation and Cybersecurity. In M. E. Realpe Díaz & A. M. González González (Eds.), *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* (pp. 15-42). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818064.01>

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

Technological convergence, where information flows are becoming more frequent every day, marks the advent of the digital revolution due to the interconnected world in which we are, with instant, permanent, and updated information. All this has produced a change in computer systems and the demand for security as a challenge that organizations and individuals face daily.

Protecting information is one of the most prominent concerns organizations have today. Due to globalization and the Internet of Things (IoT), more and more public and private entities face new threats and risks. Thus, the security policies implemented or the technological investment companies make are not enough to counteract this scourge; the personnel working in the institutions and representing the weakest link in information security must be considered.

Organizations must take a resilient position in the face of cybersecurity problems, i.e., they must anticipate the threats and risks that arise since they are becoming more varied and widespread. This makes it difficult to protect information assets and forces organizations to change their perspective regarding how to act upon it in a dynamic and uncertain world.

Information security must be incorporated into corporate strategies and tactical plans that understand an organization's business model. This understanding allows an organization to anticipate future challenges and support decision-making regarding cybersecurity issues.

This chapter offers an overview of the key concepts and ideas about strategic forecasting and foresight, the importance of raising awareness of cybersecurity in organizations, and the use of perspective to achieve an organizational culture in cybersecurity.

Strategic Forecasting and Foresight

Forecasting has long been used to describe how governments prepare for and address long-term problems. *Technology foresight* began to be used in the 1990s in Europe, although later, other countries began to address it as a policy relating to science, technology, and innovation systems (Miles, 2010).

Irvine and Martin's studies highlighted *forecasting* as the popular way to describe broad research and innovation curricula for future developments (Miles, 2010). In many cases, forecasting is conducted to anticipate the main social and future challenges, managing to support decision-making not only because it identifies technological changes but also because it involves the relevant stakeholders that will generate knowledge and innovation.

According to Könnölä et al. (2010), forecasting activities have tended to shift from focusing on positivist and rationalist technologies to recognizing broader concerns spanning the entire innovation system, taking into account social approaches, such as sustainability, security, and information society.

On the other hand, foresight plays a definitive role in organizations' decision-making since it allows organizations to prepare for the future. It identifies both promising technological paths and different stakeholders interested in anticipating and creating common actions that involve preparing for and confronting what is coming (Könnölä et al., 2010).

Foresight is thus recognized as a systematic, participatory process of brainstorming ideas that can be used in the long term for current and future decision-making and allows for strategic planning that meets organizations' objectives.

Due to the social challenges that arise every day due to technological convergence, IoT, and the digital economy, among others, research results are needed to support specific situations in decision-making. Therefore, it is necessary to consider data and studies, as they serve as a guide to prepare us to face future science, technology, and innovation challenges and make better decisions (Könnölä et al., 2010, p. 3).

Experience in the use of foresight and perspective in countries such as Japan, the Netherlands, the USA, Spain, and the United Kingdom demonstrates that their systematic incorporation in science and technology processes has improved strategies and served as a guide for decision-making in implementing policies in both public and private organizations. This reveals the importance of foresight for an organization since the studies in this regard make it possible to minimize many

risks brought by technology and digitalization and, generally, achieve information security, which is one of the challenges of organizations (Miles, 2010, pp. 7–8).

Regarding cybersecurity awareness, foresight is required to predict the future since new risks and threats arise daily and as a tool that allows organizations to be resilient against challenges and implement better strategies.

Likewise, information insecurity will continue to be an imminent problem for governments due to connectivity and the need to be permanently informed, so the challenges will continue to be huge for researchers and those in charge of the security of information assets.

Strategic Foresight: Importance for the Future of Organizations

Organizations increasingly use strategic foresight because it gives them a vision of the future and allows for continuous improvement in processes to counteract the risks and threats that a lack of foresight may cause.

Companies should consider the strategy as a whole and begin to implement or correct it gradually, depending on their pace of adaptation. According to Mintzberg et al. (1998), ten schools categorize the strategy into three main groups. The first, known as *prescriptive*, focuses on formulating strategies before considering their conception. The second group, comprised of six schools, describes procedures, prioritizes content and positioning, and transforms the strategy into something different, systematic, and formal. Finally, the school of knowledge emerges, which seeks to use the tools of cognitive psychology to understand the strategist's mind.

One of the strategy's main objectives is to resolve the significant challenges and problems that may arise in organizations in the future. This does not mean that by implementing or modifying a strategy, we are already exempt from a threat or danger; instead, many possible risks are minimized. Following Mintzberg et al. (1998), "A strategy moderates the ability to respond to changes and modifications in the environment; that is, it is a fundamental element that forces you to go straight and does not allow you to look away" (p. 4).

To implement a good strategy, we must, however, review its importance for organizations. For this reason, Mintzberg et al. (1998) describe the role of strategy and its advantages in four points: 1) as guidance, since it serves as a compass for an organization; 2) as a concentration of efforts, since it allows the concentration of

activities; 3) as meaning to the organization, since it distinguishes it from the others, and 4) as a source of coherence, since it helps to understand the environment and with this the implementation of actions that respond to it.

Therefore, when implementing strategies, organizations must consider them as a whole, not at their convenience or as best suited to the organization. For the school of culture and spirit, strategies are unique perspectives from a person's point of view or organizational culture and, therefore, each one is different; that is, they cannot be compared with other strategies since these are derived and born from personal adaptation processes and are the result of individual creative efforts (Mintzberg et al., 1998).

Strategies for a Culture of Information Security

This section explores the essence of cybersecurity and digital transformation: the organizational culture surrounding information security. According to Beaver (2018), adequate security is not simply a matter of tools and technology but also attitudes, behaviors, and awareness within the organization. Here is where strategies to foster a safety culture become crucial (Spafford, 2006).

The organizational culture of information security (COSI, by its Spanish acronym) is a relevant issue that allows companies to increase their resistance to cyberattacks. Although it is a topic that must be studied, public and private companies still need to give it the relevance it requires (Cano, 2016).

The organizational culture works toward protecting information, which ceases to be just another resource for companies and becomes a vital strategic asset for decision-making. Cybersecurity is a risk management problem and must be addressed from a strategic, economic, and reactive perspective. It must involve all organization members and be a cross-cutting process for all areas of the entity. Protecting the assets of entities from cybercrimes is not an option, but rather a key element for the development of an organization (Organization of American States [OAS], 2017).

According to Sechin (as cited in Cano, 2015), "An organizational culture is built from what people believe, what persons do, and what individuals see." To build a culture of information security, it is necessary to study people's behavior since this reflects how they act on security issues, the responsibility with which they face them, and, in many cases, the level of knowledge they have regarding cybersecurity. This analysis seeks to coordinate the relationship between people

and information, the responsibility that each person has from the role they play in this asset, and the value it has for the strategic and missional fulfillment of each entity, seeking not only compliance with strategies and regulations implemented by the company but also ownership for the protection of information.

It is known that when prospective strategies are implemented for an organization concerning information security, these cannot be addressed 100% since new threats and risks emerge every day due to technological evolution and their convergence. Here is where information security managers begin to assess "which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach" (OAS, 2017, p. 24). Once these aspects are analyzed in terms of the cost-benefit they can generate for the company, it is good to make this decision. Based on the above, some strategies that support the culture of information cybersecurity are described below.

Importance of Information Security

Information security is essential in any organization to ensure the protection of confidential data and avoid potential financial loss or reputational damage. In the Information Age, when information is exposed to various risks and threats, such as data theft or cyberattacks, it is crucial to have adequate security strategies and measures. Information is a valuable asset that can provide competitive advantages, so its protection becomes a priority to ensure business continuity. Implementing security policies and procedures, as well as staff training and awareness, are crucial to achieving an influential information security culture. In addition, it is important to continually evaluate and improve the security system to adapt to technological changes and new threats that may arise.

Identification of Risks and Vulnerabilities

Identifying risks and vulnerabilities is a fundamental step to achieving an influential information security culture. This process allows us to identify the possible dangers our organization is exposed to and the weaknesses in our systems and processes that malicious actors could exploit. To carry out this task, both internal and external risk assessments must be conducted to detect possible threats and vulnerabilities. Security analysis tools and techniques like penetration testing and vulnerability scans can also help us identify potential system gaps. Once the risks and vulnerabilities have been identified, the necessary measures can be

implemented to mitigate them and guarantee the protection of an organization's information (Cando, 2024; Castillo, 2023).

Development of Security Policies and Procedures

Developing security policies and procedures is critical to establishing an organization's strong information security culture. These policies must be designed comprehensively and consider all relevant aspects, such as the classification of information, access and protection of assets, password management, and security in the use of mobile devices. Furthermore, the procedures must be clear and detailed, specifying the technical and operational actions necessary to guarantee information security. These documents must be communicated and distributed to all members of the organization, who must commit to complying with the established policies and procedures. In addition, a periodic review and update process of these policies and procedures must be established to ensure they align with new threats and changes in the security environment (Montalbán et al., 2020; Muñoz, 2021; Valencia, 2021).

Staff Training and Awareness

Staff training and awareness are fundamental aspects of achieving a culture of information security. It is vital to provide all employees with adequate training on computer security issues, including basic concepts of data protection, secure password management, prevention of cyberattacks, and good practices in using technological systems and resources. Besides, it is important to raise awareness about the rights and responsibilities of staff regarding information security, promoting the relevance of maintaining data confidentiality, integrity, and availability. To ensure adherence to these measures, regular and updated training programs must be carried out, including periodic assessments to measure the level of knowledge and promote continuous improvement in the safety culture (Arpi & Cajamarca, 2023; Barcia, 2023; Fong & Bayona, 2022).

Evaluation and Continuous Improvement of the Security System

The evaluation and continuous improvement of the information security system are essential to guarantee its effectiveness and efficiency over time. To do this, it is necessary to perform periodic audits to identify possible failures or weaknesses

in the system. These audits must be performed internally and externally by professionals with experience in information security. Internationally recognized standards, e.g., ISO 27001, must be followed to assess compliance with the controls and security measures implemented. Furthermore, it is important to consider emerging threats and vulnerabilities and adapt the security system accordingly. For continuous improvement, indicators and metrics must be established to measure the system's effectiveness and take corrective actions when deviations are detected. It is also advisable to conduct security drills and tests regularly to evaluate the response capacity and detect possible areas for improvement. In summary, the evaluation and continuous improvement of the information security system is an essential process to maintain the protection of assets and guarantee the confidentiality, integrity, and availability of information (Bedoya & Patiño, 2023; Sánchez et al., 2023; Sepúlveda & Medina, 2024).

Finally, individuals are fundamental for the success of organizational safety culture programs since each one plays a role that contributes positively or negatively to the organization. This is why awareness-raising programs are important for companies since they reduce the risks and vulnerabilities that entities may suffer.

Philosophy of Cybercrime

Cybercrime is a criminal activity carried out in the digital sphere, using information and communications technologies as tools to commit crimes (Saín, 2018). These crimes may include the theft of personal or financial data, forgery of identities, unauthorized access to computer systems, and dissemination of illegal content. Cybercrime is characterized by its global nature, since it can be perpetrated from anywhere in the world, and by its capacity to cause large-scale damage both at the individual and societal levels.

Cybercrime has several characteristics that distinguish it from other types of crimes. First, it is committed covertly, taking advantage of the relative anonymity that the internet provides. Second, cybercrime is highly sophisticated, requiring specialized information technology knowledge and advanced technical skills. Third, cybercrime is a constantly evolving phenomenon, with cybercriminals adapting their methods and techniques to circumvent security measures. Finally, cybercrime can have an almost unlimited global reach since the internet allows criminals to operate in different countries and attack people worldwide (Incibe-Cert, 2020).

Cybercrime has a significant impact on society on multiple levels. At an individual level, it can cause personal and financial data loss and deterioration of online privacy and security. At the enterprise level, cybercrime can result in security breaches, loss of customers, and damage to the reputation of organizations. At the societal level, cybercrime can affect trust in institutions, undermine the digital economy, and generate significant costs for governments and citizens (Cano, 2011). Furthermore, cybercrime can contribute to the spread of misinformation, widening the digital divide and exacerbating inequality. Therefore, it is important to address cybercrime effectively to protect individuals and safeguard the well-being of society as a whole.

The philosophy of cybercrime analyzes and reflects on the fundamental aspects related to this criminal phenomenon. Different elements are addressed, such as the origin and evolution of cybercrime, the motivations of cybercriminals, the ethics and morals involved in these practices, and the philosophical implications arising from this type of crime (Creese et al., 2020). With a critical and reflective approach, we seek to understand the ethical, moral, and philosophical dimensions of cybercrime and its influence on today's society (Sáinz, 2016).

The fight against cybercrime faces constant challenges due to rapid technological advancement and the sophistication of the techniques used by cybercriminals. The increased connectivity and the digitalization of various areas of society provide new opportunities to commit online crimes. Cybercriminals are constantly adapting, improving their techniques, and exploiting emerging vulnerabilities. Moreover, anonymity and the lack of a single jurisdiction make it difficult to chase and capture those responsible (Saín, 2018). Other challenges include a lack of cybersecurity awareness and training in various sectors, the shortage of cybersecurity experts, and the need for financial resources to combat cybercrime effectively. Overcoming these challenges requires a collective response and constant adaptation to new threats and scenarios to fight them.

With the development of the internet, favorable conditions have been created for those who pursue personal interests at the expense of network users. The effects have common characteristics, such as a serial killer environment and low levels of harassment. Crime can be committed anywhere in the world with internet access. It can affect organizations or individuals anywhere, giving criminals a high-impact, easy-to-implement, anonymous level of risk, efficiency, and effectiveness. In some cases, the perpetrator does not need in-depth knowledge to commit a cybercrime. In this regard, the World Economic Forum lists infrastructure failures,

cyberattacks, and fraud or data theft (which involves the theft of personal data) as the top ten global threats (World Economic Forum [WEF], 2013).

Cybersecurity Challenges

Cyber threats are constantly evolving and represent an increasing challenge to digital security. The attack techniques used by cybercriminals are increasingly sophisticated and can affect both individuals and organizations (Incibe-Cert, 2020). Some of the most common cyber threats include phishing, malware, ransomware, and denial of service attacks. These attacks can have devastating consequences, including the loss of sensitive data, theft of personal or financial information, and damage to a company's reputation. To address these threats, it is essential to have adequate security measures in place, such as antivirus software, two-factor authentication, and cybersecurity education, to ensure the protection of digital systems and data (Mijares, 2020).

Vulnerabilities in digital infrastructures pose a significant cybersecurity challenge. These vulnerabilities can arise for various reasons, such as using obsolete or outdated systems, lack of security patches, inadequate implementation of protective actions, and unawareness of cyber threats. Additionally, digital infrastructures are often interconnected, meaning that the vulnerability of one system can affect other systems. This highlights the importance of implementing robust and up-to-date security measures at all layers of the digital infrastructure, from servers and networks to end devices (Pérez et al., 2012). It is also crucial to conduct periodic vulnerability assessments and make corrections to mitigate risks and strengthen security in digital infrastructures.

Data protection strategies play a fundamental role in cybersecurity. To ensure information security, it is essential to implement measures such as data encryption, firewalls and intrusion detection systems, and robust password policies. In addition, it is necessary to make regular backups and have an incident response plan that allows us to act quickly and effectively in the event of any eventuality. Other strategies include network segmentation, two-factor authentication, and constant user activity monitoring. Implementing identity and access management tools can also help prevent unauthorized system access. In summary, having a comprehensive data protection strategy is essential to mitigate risks and protect information from potential cyberattacks (IT Trends, 2019).

The role of governments in cybersecurity is fundamental to protect and guarantee the security of citizens and organizations against cyber threats. Governments are responsible for establishing and enforcing laws and regulations that promote the protection of information systems and data privacy. In addition, they must encourage cooperation and collaboration between the public and private sectors, facilitating information exchange and developing good cybersecurity practices (Ibarra & Igartua, 2018). Governments must also invest in the education and training of cybersecurity professionals to prepare them for new technological challenges and promote the research and development of advanced technologies and tools that can help prevent and detect cyberattacks. In short, the role of governments in cybersecurity is essential to protect society and foster a safe and trustworthy digital environment (Evans & Farrell, 2020).

Cybersecurity education and awareness are critical in protecting individuals and organizations from cyber threats. Through educational programs and awareness campaigns, we seek to inform people about how they can be victims of cyberattacks and how they can prevent them. These programs include teaching safe practices in using the internet, email, and social media and promoting the importance of keeping operating systems and security software up-to-date. The risks associated with using weak passwords and sharing personal information online should also be highlighted. Cybersecurity awareness also extends to companies, encouraging the implementation of internal security policies and staff training and creating an organizational culture that prioritizes the protection of digital information (Deloitte et al., 2013). Some examples of these challenges are:

Advances and Policies in the United States

Various initiatives and legislation have been implemented in the USA to address cybersecurity challenges. A notable example is the Modernization of Research and Innovation Infrastructure Act (MIIRIA), which includes provisions to strengthen cybersecurity at federally funded research and development institutions. The National Cybersecurity Strategy, launched in 2018, also establishes a comprehensive framework to protect critical infrastructure and strengthen the country's cyber resilience.

Advances and Policies in the European Union

The EU has taken a coordinated approach to improving regional cybersecurity. The General Data Protection Regulation (GDPR), implemented in 2018, sets rigorous

standards for protecting personal data and forces organizations to take proactive measures to ensure data security. Furthermore, the EU Cybersecurity Strategy, launched in 2013 and updated in 2020, promotes cooperation between Member States and the private sector to address cyber threats effectively.

Advances and Policies in China

China has established several regulations and laws to strengthen its cybersecurity position. For example, the Cybersecurity Law of the People's Republic of China, implemented in 2017, establishes requirements to protect critical infrastructure and regulate the handling of personal data. Additionally, China's National Information Security Action Plan, launched in 2019, sets out goals and measures to improve cybersecurity in the country.

Advances and Policies in Japan

Japan has developed a series of initiatives to strengthen its cybersecurity capacity. Japan's Cybersecurity Strategy, launched in 2015 and updated in 2020, establishes objectives and measures to protect critical infrastructure and promote collaboration among the Government, the private sector, and academia. Additionally, Japan's Act on the Protection of Personal Information, enacted in 2005 and amended in 2015, establishes standards for the secure handling of personal data.

Advances and Policies in Australia

Australia has introduced several initiatives to strengthen its cybersecurity capacity. For example, the Australian Government launched the Australian Cybersecurity Strategy in 2020, which includes significant investments in cybersecurity infrastructure and cyber defense capabilities. Australia's Notifiable Data Breaches scheme, implemented in 2018, also requires organizations to notify authorities and affected individuals during a data security breach.

Weak Links

Nowadays, cybersecurity has become an issue of vital importance for organizations. In addition to protecting confidential company information and customer data, cybersecurity also plays a critical role in protecting against external

threats. The increasing dependence on technology in the business environment has increased organizations' vulnerability to cyberattacks, highlighting the need to implement appropriate security measures. A lack of cybersecurity can have devastating consequences, such as theft of sensitive information, disruption of business processes, and loss of customer trust. Therefore, organizations must recognize the importance of investing in cybersecurity to protect their assets and maintain business continuity.

Organizations face several common cybersecurity threats. One is phishing, in which attackers try to obtain confidential information by posing as trusted entities. There are also malware attacks, which can infect the organization's systems and compromise data integrity. Another type of threat is ransomware, in which cybercriminals block access to files and demand a ransom for their release. Additionally, brute force attacks are common, using programs that attempt to guess passwords to access systems or accounts. Finally, organizations should also be concerned about denial-of-service attacks, where an attempt is made to overload a website or service to make it inaccessible to legitimate users. Organizations must be prepared and take preventive measures to mitigate these threats and protect their systems and data.

Several factors can weaken cybersecurity in organizations. One of them is the absence of cybersecurity awareness and training on the part of employees. Workers often ignore good security practices or fall into phishing traps and other attacks. Another factor is the need to update the systems and applications used. If organizations do not install the latest security patches and updates, they leave vulnerabilities exposed to attacks. Additionally, the lack of clear and consistently applied security policies and procedures can weaken an organization's cyber protection. Establishing security rules and guidelines and ensuring compliance is necessary to avoid security breaches. In brief, ignorance, a lack of updates, and the absence of clear policies weaken cybersecurity in organizations.

Weak links in organizations' cybersecurity can have serious consequences. One of the main repercussions is the risk of suffering a cyberattack. Hackers can use these vulnerabilities to infiltrate the system and access sensitive information. This can result in the theft of data, such as passwords, credit card numbers, or personal information of customers and employees. Weak links can also facilitate the spread of malware, which can impact system performance and cause financial damage. On the other hand, organizations that do not adequately manage information security can face serious legal consequences and reputational damage in the event of data breaches. In short, weak links in cybersecurity are a severe threat that can have financial, legal, and reputational repercussions for organizations.

To improve cybersecurity in organizations, adopting a series of measures and solutions is essential. First of all, it is advisable to implement a continuous network monitoring system in order to detect any suspicious activity or intrusion attempt. Second, there should be a cybersecurity education and awareness program in place, providing training to all organization members so that they understand threats and how to respond to them. Third, it is necessary to establish clear and rigorous password management policies, encouraging strong and periodically updated passwords. Another critical measure is the implementation of two-factor authentication systems, which provide an additional layer of protection. Finally, it would be best to have a response plan for security incidents, which allows a quick and efficient reaction to possible attacks or security breaches. These improvements and solutions are essential to strengthen organizations' cybersecurity and protect data and systems integrity.

Cyber Resilience and Cybersecurity Awareness

In today's world, where technology and interconnectivity play an increasingly important role in our society, *cyber resilience* and *cybersecurity awareness* are two fundamental concepts. In this chapter, both terms are analyzed in detail, exploring their importance and the strategies that can be implemented to strengthen security in the digital environment. In addition, we examine the available tools and technologies that can contribute to cyber resilience, as well as the conclusions reached after the study. This work aims to provide solid knowledge on such relevant topics and encourage greater awareness regarding cybersecurity.

Importance of Cyber Resilience

Cyber resilience is a fundamental aspect of today's cybersecurity. It refers to an organization's ability to resist, adapt, and recover from cyber incidents and attacks. It is essential to ensure business continuity and protect confidential information. Cyber resilience is vital because it allows us to reduce risks and mitigate the possible negative consequences of a cyberattack. Besides, it guarantees the ability to respond quickly and efficiently to potential incidents, thus minimizing the impact on an organization. Implementing cyber resilience strategies strengthens system security and maintains the trust of customers and business partners.

Cybersecurity Awareness Strategies

Cybersecurity awareness strategies are essential to educate and make people aware of the risks and threats in the digital world. One of the most effective strategies is to carry out training and training programs that provide practical knowledge about good computer security practices. These programs may include talks, workshops, and courses that address topics such as secure password use, identifying suspicious emails and links, and protecting personal information. Another essential strategy is the creation of awareness campaigns that reach a broad audience through the media, social media, and other dissemination channels. These campaigns can use clear and direct messages to inform about risks and promote responsible use of technology. Cyberattack simulations can also be implemented to evaluate response capacity and raise awareness of the importance of staying alert to potential threats. In short, cybersecurity awareness strategies are essential to foster a culture of security in society and reduce the incidence of cyberattacks.

In conclusion, cyber resilience is vital today, where cyberattacks are increasingly frequent and sophisticated. Cybersecurity awareness strategies are essential to protect organizations from possible threats and minimize risks. Furthermore, using appropriate tools and technologies to strengthen cyber resilience is crucial. These tools may include intrusion detection and prevention systems, data encryption, and backup and recovery systems. Organizations must invest in training and constant updating to be prepared for any contingency. Cyber resilience is not only about resisting and recovering from attacks but also about learning from them and improving security in the future.

Public-Private Cooperation in Cybersecurity and Culture

Cooperation between the public and private sectors in cybersecurity is vital due to the growing challenges of protecting information and digital systems. Both sectors possess unique knowledge and resources that, when combined, can significantly strengthen cybersecurity defenses. The public sector has experts in policy and regulatory frameworks, while the private sector brings expertise in technology and adaptability. Additionally, collaboration enables timely sharing of threat and vulnerability information, facilitating early detection and response to security incidents. The public and private sectors can effectively address cybersecurity challenges and protect critical data and systems by working together.

Collaboration between the public and private sectors in cybersecurity has numerous benefits. Firstly, it combines both sectors' experience and knowledge, enabling us to address computer security challenges more effectively. Secondly, this collaboration promotes interoperability and information exchange among organizations, allowing for a faster and more coordinated response to cyber threats. Thirdly, public-private partnership in cybersecurity strengthens the protection of critical infrastructures by pooling resources, technologies, and good practices. Finally, this collaboration can boost economic development by encouraging innovation and job creation in the field of cybersecurity.

One of the main challenges in cybersecurity cooperation is the need for more mutual trust between the public and private sectors. There is a reluctance on the part of private companies to share sensitive information with government authorities for fear of data leaks or being used against them. On the other hand, public institutions may need more support in acting due to legal and bureaucratic restrictions. The lack of common standards and protocols also makes communication and collaboration between both sectors difficult. The rapid evolution of information and communication technologies represents a constant challenge as cyber threats and vulnerabilities evolve quickly and complexly. Therefore, overcoming these challenges and promoting new forms of cooperation in cybersecurity that allow for an effective and coordinated response to digital threats is necessary.

Promoting a culture of cybersecurity is essential to protect information and maintain security in the digital sphere. To this end, it is necessary to make people aware of the risks and good practices in cybersecurity. This involves providing cybersecurity training and education at the individual and organizational levels. Organizations should implement awareness programs that include the importance of strong passwords, phishing detection and prevention, and adequate protection of sensitive data. Furthermore, it is essential to foster a general culture of cybersecurity in society, promoting responsibility and the safe use of digital technologies.

Taking action is essential to promote cooperation and a cybersecurity culture. First of all, it is necessary to encourage cybersecurity training for both the public and private sectors, with the aim of having specialized personnel aware of the risks. Likewise, awareness-raising programs should be established aimed at society in general so that citizens are informed and adopt safe practices in their digital lives. It is important to facilitate collaboration and the exchange of information between both parties by creating cooperation platforms and networks. These platforms will help share good practices, knowledge, and security alerts in an agile and effective way. Lastly, incentives and recognition should be established for those

organizations and companies that demonstrate a significant commitment to cybersecurity and foster a culture of information protection. All these measures will strengthen cooperation and cybersecurity culture in the public and private spheres.

Experiences and Appropriate Practices

This section presents various successful experiences in the field of cybersecurity. Actual cases are addressed in which companies and institutions have implemented adequate measures to protect their digital infrastructure and safeguard their data confidentiality, integrity, and availability. It analyzes how these organizations have managed to confront cyber threats and strengthen their security by adopting advanced technologies, implementing robust security policies, training staff, and collaborating with cybersecurity experts. In addition, this section highlights the benefits obtained from these successful experiences at the information protection, reputation, and customer trust levels. Likewise, it explores the challenges and obstacles faced during the implementation process, as well as the lessons learned that may be useful for other organizations interested in improving their digital security (Goundar et al., 2021; Pérez et al., 2018; Vial, 2019).

In the sphere of digital transformation, it is vital to follow a series of recommended practices to ensure success and maximize the benefits of this process. First, it is essential to establish a clear and defined strategy that sets the objectives and goals to be achieved with digital transformation. It is also necessary to have the support and leadership of the management team to ensure the involvement of all organization members (Schmitt, 2018). Another important aspect is to thoroughly analyze existing processes and systems, identifying areas for improvement and possible obstacles that may arise during the transformation process. It is also advisable to use technological tools and innovative solutions that facilitate the automation and optimization of processes. Finally, it is crucial to have a training and education plan in new technologies and digital skills to ensure that all organization members are prepared to adapt to changes and make the most of the opportunities offered by digital transformation (Patiño, 2018; Teslia et al., 2016).

The implementation of cybersecurity poses a series of challenges and risks that are important to take into account. Firstly, one of the main challenges is the adaptability and constant updating of security measures. Technological advances and new cyber threats demand that organizations constantly stay aware of changes and update their security systems effectively. Another challenge relates

to the need for cybersecurity awareness and education. Many employees need to learn to recognize and avoid cyberattacks, which can put company security at risk. Cybersecurity implementation can also face technical challenges, such as integrating different systems and managing data securely. It is essential to address these challenges and risks with practical strategies and prioritize the protection of organizations' digital infrastructure.

Commercial Technologies for Cybersecurity

In today's digital world, cybersecurity has become an unavoidable priority for companies and governments. With cyberattacks on the rise, the demand for advanced technologies and robust solutions to protect systems and data is higher than ever. The commercial technologies used nowadays in cybersecurity, according to Palo Alto Networks (2023), include:

Authentication and Identity Management

Technologies Used

Multi-factor authentication (MFA)—essential technology that adds layers of security by requiring multiple forms of verification before granting user access. Usage example: Financial institutions use MFA to protect user accounts by combining passwords with a temporary code sent to a user's mobile device.

Identity and access management (IAM)—solutions such as Okta or Microsoft Azure Active Directory allow organizations to manage and monitor user identities and access different corporate resources. Usage example: Companies implement IAM to ensure only authorized employees can access critical systems and sensitive data.

Encryption

Technologies Used

Encryption of data at rest and in transit—using algorithms such as AES and RSA to encrypt data, ensuring that information is inaccessible during transfer or storage. Usage example: Cloud storage services use encryption to protect user data stored on their servers.

Network Security

Technologies Used

Next-generation firewalls and intrusion prevention systems (IPS)—tools like Cisco Firepower or Palo Alto Networks monitor network traffic and block suspicious activity. Usage example: Organizations use IPS to detect and prevent automated attacks and other network threats.

Virtual private network (VPN)—allows users to establish a secure, encrypted connection to a corporate network from a remote location. Usage example: During remote work, employees use a VPN to access internal company resources securely.

Security Analysis and Incident Response

Technologies Used

Extended detection and response (XDR) tools—platforms such as SentinelOne or CrowdStrike provide complete visibility across endpoints, networks, and servers, facilitating rapid threat detection and automated response. Usage example: Technology companies deploy XDR to detect anomalous behavior in real time and respond to security incidents in an automated manner.

Emerging Technologies: Their Impact on Cybersecurity for Digital Transformation

Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) transforms cybersecurity, offering new ways to detect and respond to threats in real time. AI can analyze large volumes of data to identify suspicious patterns and behaviors, enabling faster and more accurate threat detection than traditional methods. Additionally, AI systems are used to automate responses to security incidents, reducing the burden on cybersecurity teams and improving the effectiveness of responses (Morgan, 2021).

Internet of Things

The Internet of Things (IoT) represents a significant challenge for cybersecurity due to the large number and diversity of connected devices, many of which

need to be designed with security as a priority. This increases the attack surface and exposes unique vulnerabilities in corporate and consumer networks. Cybersecurity technologies for IoT must address everything from device security to network protection and transmitted data, ensuring the integrity of increasingly interconnected systems (Weber, 2023).

Cloud Computing

Cloud computing has allowed companies to scale resources and improve efficiency, but it has also introduced new cybersecurity risks, such as misconfiguration of cloud environments that can expose sensitive data. Cloud security solutions, such as web application firewalls and identity and access management tools, are crucial to protecting data hosted on cloud services (Jackson, 2022).

Big Data and Cybersecurity

Big data offers significant opportunities to improve cybersecurity by analyzing massive data sets to detect anomalies and attack trends. However, it also poses challenges in protecting and managing these large volumes of data. Emerging big data technologies require robust security measures, including advanced encryption and specific solutions for large-scale data protection (Thompson, 2023).

To illustrate the concepts described, we present some diagrams explaining each emerging technology mentioned and their impact on cybersecurity for digital transformation. These diagrams include details on AI, IoT, cloud computing, and big data, each highlighting how these technologies strengthen security in a digital environment. The description and use of each one are presented in Table 1.

Table 1. Description and Use of Emerging Technologies in Digital Transformation

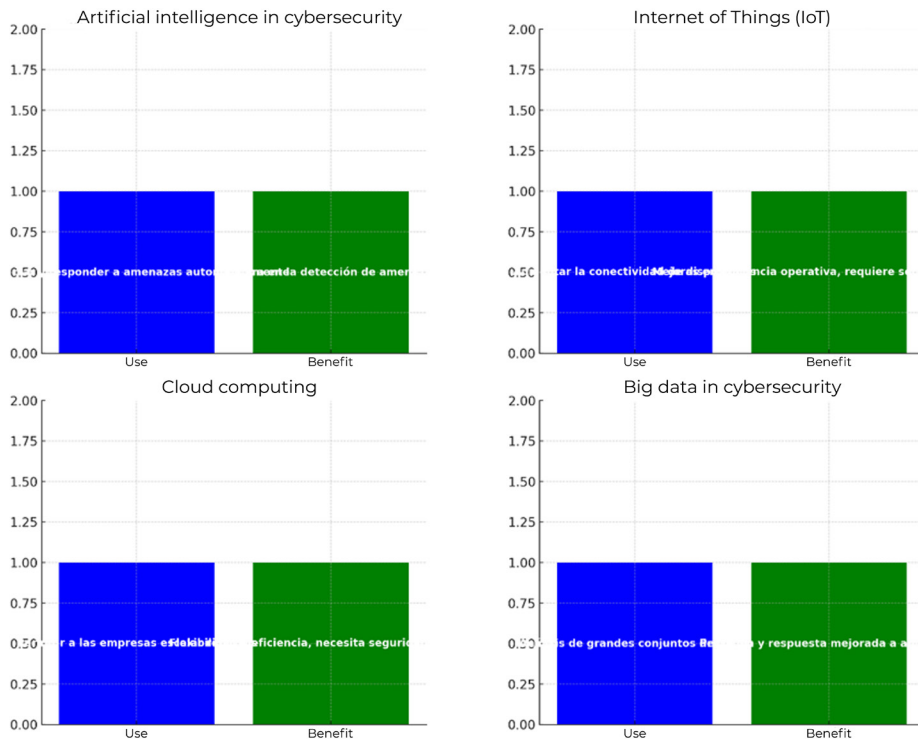
Technology	Use	Benefit
AI in cybersecurity	Automatically detects and responds to threats by analyzing large volumes of data to identify anomalous behavior patterns	Improves speed and accuracy in threat detection
IoT	Increases device connectivity but increases the attack surface due to the diversity and number of connected devices	Improves operational efficiency but requires robust security measures to protect corporate and consumer networks
Cloud computing	Allows companies to scale resources and improve efficiencies but also introduces new risks, such as misconfiguration that can expose sensitive data	Flexibility and efficiency with the need to implement specific security solutions for the cloud

Big data	Analyzes extensive data sets to detect threats and anomalies, addressing challenges to protect and manage that data	Improved ability to anticipate and respond to cyber threats by identifying trends from large volumes of information
-----------------	---	---

Source: Own elaboration.

Figure 1 shows the impact of emerging cybersecurity technologies on digital transformation. Each diagram highlights the main application and benefit of the following technologies: 1) AI in cybersecurity: used to automatically detect and respond to threats, improving the speed and accuracy of detection; 2) IoT: increases device connectivity, requiring robust security measures to protect expanded networks; 3) cloud computing: allows companies to scale resources, needing specific security solutions to protect data in cloud environments, and 4) big data in cybersecurity: uses the analysis of large volumes of data to detect trends and threats, improving forecasting and response capacity.

Figure 1. Diagrams of the Impact of Emerging Technologies on Cybersecurity



Source: Own elaboration.

The diagrams in Figure 1 use bars to represent two main categories: “use” and “benefit” of each technology. The function of each axis in the diagrams is as follows:

X-axis (horizontal)—represents the categories compared for each technology. In this case, the X-axis has two categories labeled “use” and “benefit.” These categories describe how each technology is used in cybersecurity and what primary benefit it brings.

Y-axis (vertical)—shows a measurement scale for the compared values. In the diagrams provided, the Y-axis does not represent a traditional quantitative scale but is used more as a method to organize information visually. The bars are the same height since they aim to highlight the textual information within them, not measure quantities.

Each bar in the diagram is colored differently to distinguish between the use and benefit of each technology. The information in the bars provides specific details on how each technology is applied in the cybersecurity context and the benefits it offers. This helps to visually understand the contribution of each technology to digital security in the digital transformation era.

Conclusions

Foresight studies are essential for making policies and strategies that minimize the risks that may arise in organizations and allow better decisions to be made in the future. To achieve this, interactive work must be conducted in which all stakeholders are involved, futuristic projects are built, and existing processes are improved.

Cybersecurity awareness is an ongoing activity that should begin at the primary education level and involve all citizens. This will undoubtedly benefit people and the workplace, thus creating a cyber-resilient nation.

The use of strategic foresight is the best option for entities to be prepared for future changes, both social, political, and economic, and to be able to respond to them. That is, the formulation of strategic plans allows companies to respond resiliently to possible changes that may arise. The above does not mean that strategic foresight will solve the future, but it will allow us to minimize many risks and threats that an organization may suffer.

This is where the generation of knowledge and innovation plays a vital role in cybersecurity forecasting and the integration of all the actors involved so that this planning leads to improvements in processes and, in the case of cybersecurity,

serves as a guide to minimizing the risks and threats that emerging technologies bring with them.

The construction of an entity with these particularities poses apparent challenges. First, management must provide specialized resources, such as public communication, cybersecurity, and legal advice. Second, it requires making and implementing agreements. Lastly, adequate investment is needed to ensure the success of this company.

Despite the challenges involved, the long-term benefits of this initiative are evident. An example of this is the approach adopted by the European Union to promote investment in R&D&i within the framework of Horizon 2020. There are several public-private partnerships (PPP), especially in cybersecurity, to direct investment toward the interests and needs of production sectors.

Nonetheless, individual knowledge of cybersecurity is not enough. People must engage effectively with their companies and nations. In the workplace, companies and organizations must provide employees with a sense of belonging, job security, group identity, and even a shared purpose, in addition to offering added values beyond direct financial remuneration. At the national level, it is essential to inform citizens that their cybersecurity contributes to national security.

In conclusion, to improve our global cybersecurity culture, it is essential to 1) take into account the human factor, 2) have the institutional support and resources necessary to implement the required plans and coordinate them with state interests, and 3) bring together all stakeholders in a public-private partnership to define the most appropriate work strategies that guarantee success.

Digital transformation and cybersecurity will continue to evolve in the future as technologies advance and cyber threats become more sophisticated. Organizations must adapt to new trends and challenges to protect their digital infrastructure. Two critical areas in this evolution are artificial intelligence (AI) and machine learning (ML) in digital security. AI and ML enable cybersecurity solutions to be more proactive and efficient by detecting and mitigating threats in real time. These technologies can analyze large amounts of data in an automated manner, identifying patterns and anomalies to anticipate future attacks. Their application to digital security will be fundamental in the fight against cybercriminals.

Artificial Intelligence and Machine Learning in Digital Security

Artificial intelligence (AI) and machine learning (ML) have revolutionized digital security. These technologies allow cybersecurity systems to learn and adapt

autonomously without constant human intervention. AI and ML analyze real-time data, identify anomalous patterns and behaviors, and generate alerts for potential threats. Additionally, they can predict and anticipate future attacks, providing greater protection in a constantly evolving cyber environment. These advanced capabilities make AI and ML essential tools for digital security, enabling early detection and rapid response to threats.

Internet of Things and Its Impact on Cybersecurity

IoT is a trend in digital transformation that is producing a significant impact on cybersecurity. With the increasing interconnection of devices and systems, the need arises to protect computer equipment and everyday objects that are part of daily life. IoT devices are exposed to cyber threats, such as unauthorized access, data interception, or remote tampering. Appropriate security measures such as data encryption, strong authentication, and network segmentation must be implemented to mitigate these risks. Furthermore, monitoring and managing the security of IoT devices becomes essential to ensure a secure and reliable digital transformation in a connected environment.

The cybersecurity technologies discussed are critical to protecting critical infrastructure and valuable data in today's digital environment. Proper implementation can mean the difference between security and vulnerability in the ever-evolving threat landscape.

References

- Arpi-Saquipay, W. A., & Cajamarca-Criollo, O. A. (2023). Análisis de riesgos de seguridad de la información en una Institución de Educación Superior en Ecuador, basado en la Norma ISO 27002 Anexo A dominio 7. *MQRInvestigar*, 7(3), 2793-2808. <https://doi.org/10.56048/MQR20225.7.3.2023.2793-2808>
- Banco Interamericano de Desarrollo. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. Banco Interamericano de Desarrollo; Organización de Estados Americanos. <https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>
- Barcia Baque, G. A. (2023). *Implementación del estándar ISO/IEC 27001 para la seguridad de la información en la Unidad Educativa Fiscal Cultura Machalilla* [Bachelor's thesis, Universidad Estatal del Sur de Manabí]. Repositorio UNESUM. <https://repositorio.unesum.edu.ec/bitstream/53000/5917/1/BARCIA%20BAQUE%20GABRIEL%20ALEXANDER.pdf>
- Bedoya Velásquez, J. E., & Patiño Castrillón, J. I. (2023). *Plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales en una empresa* [Bachelor's thesis, Tecnológico de Antioquia]. Repositorio TDEA. <https://n9.cl/25ntkg>
- Cando Cando, E. D. (2024). *Propuesta de mejora de seguridad de la información digital a desarrollarse en el centro de mediación Online Dispute Resolution Quito-Rumipamba, Ecuador* [Master's thesis, Escuela de Posgrados Newman]. Repositorio EPNEWMAN. https://repositorio.epnewman.edu.pe/bitstream/handle/20.500.12892/929/rev_trabajo_obtencion_de_grado_edwin_daniel_cando_cando_epnewman_invest_aplicada.pdf?sequence=1&isAllowed=y
- Cano, J. (2011). Ciberseguridad y ciberdefensa: Dos tendencias emergentes en un contexto global. *Sistemas*, (119), 4-7. <https://acis.org.co/archivos/Revista/119/Editorial.pdf>
- Cano, J. (2015, 13 de diciembre). Cultura organizacional de seguridad de la información. Más allá de las implementaciones tecnológicas. <https://insecurityit.blogspot.com/2015/12/cultura-organizacional-de-seguridad-de.html>
- Cano, J. (2016). Modelo de madurez de cultura organizacional de seguridad de la información: Una visión desde el pensamiento sistémico. In P. Ll. Ferrer Gomila & M. F. Hinarejos Campos, *Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información* (pp. 24-29). https://www.researchgate.net/publication/309717795_Modelo_de_madurez_de_cultura_organizacional_de_seguridad_de_la_informacion_Una_vision_desde_el_pensamiento_sistemico-cibernetico
- Castillo Accarapi, W. (2023). *Sistema de gestión de la seguridad de la información utilizando la metodología Magerit en las redes informáticas de la Empresa Electronic Mihaba* [Bachelor's thesis, Universidad Andina Néstor Cáceres Velásquez]. Repositorio UANCV. <https://repositorio.uancv.edu.pe/server/api/core/bitstreams/3142acc5-a69d-4fb8-8109-8705189e6ec0/content>
- Cisco. (2023). *Cisco Firepower*. <https://www.cisco.com/>
- Evans, M., & Farrell, P. (2020). Barriers to integrating Building Information Modelling (BIM) and lean construction practices on construction mega-projects: A Delphi study. *Benchmarking: An International Journal*, 28(2), 652-669. <https://doi.org/10.1108/BIJ-04-2020-0169>

- Fong, N., & Bayona-Oré, S. (2022). Consideraciones para el cumplimiento de la política de seguridad de la información. *Revista Ibérica de Sistemas e Tecnologías de Informação*, (E51), 528-539.
- Fundación Telefónica. (2016). *Ciberseguridad, la protección de la información en un mundo digital*. Planeta.
- Goundar, S., Avaniya, J., Sunitha, G., Madhavi, K. R., & Bhushan, S. B. (2021). *Innovations in the Industrial Internet of Things (IIoT) and Smart Factory*. IGI Global.
- Ibarra, D., Ganzarain, J., & Igartua, J. I. (2018). Business model innovation through industry 4.0: A review. *Procedia Manufacturing*, (22), 4-10. <https://doi.org/10.1016/j.promfg.2018.03.002>
- Instituto Nacional de Ciberseguridad [INCIBE-CERT]. (2020). Incibe-Cert. <https://www.incibe-cert.es/>
- itTrends. (2019, 29 de marzo). Crecen los ataques cibernéticos, especialmente los destinados a Lot. IT <https://www.ittrends.es/seguridad/2019/03/crecen-los-ataques-ciberneticos-especialmente-los-destinados-a-io>
- Könnölä, T., Scapolo, F., Desruelle, P., & Mu, R. (2010). Foresight tackling societal challenges and implications on policy-making. *Futures*, 43(3), 252-264. <https://doi.org/10.1016/j.futures.2010.11.004>
- Microsoft. (2023). *Azure Active Directory*. <https://azure.microsoft.com/en-us/services/active-directory/>
- Mijares, V. M. (2020). Filling the structural gap: Geopolitical links explaining the South American Defense Council. *Colombia Internacional*, (101), 3-28. <https://journals.openedition.org/colombiaint/4185>
- Miles, I. (2010). The development of technology foresight: A review. *Technological Forecasting and Social Change*, 77(9), 1448-1456. <https://doi.org/10.1016/j.techfore.2010.07.016>
- Mintzberg, J. L., Lampel, J., & Ahlstrand, B. (1998). La estrategia y el elefante: una síntesis de las más célebres escuelas de estrategia, concebida para aplicar lo mejor de cada una. *Gestión*, 3(4), 24-34. <http://planuba.orientaronline.com.ar/wp-content/uploads/2009/09/02b-mintzberg-la-estrategia-y-el-elefante.pdf>
- Mitrovic, Z., Taylor, W., Mymoena, S., Claassen, W., & Wesso, H. (2013). E-social Astuteness skills for ICT-supported equitable prosperity and a capable developmental state in South Africa. *International Journal of Education and Development Using Information and Communication Technology*, 9(3), 103-123. <https://files.eric.ed.gov/fulltext/EJ1071374.pdf>
- Muñoz Campuzano, P. S. (2021). Modelos de seguridad para prevenir riesgos de ataques informáticos: Una revisión sistemática. [Bachelor's thesis, Universidad Politécnica Salesiana]. Repositorio UPS. <https://dspace.ups.edu.ec/bitstream/123456789/20932/1/UPS-GT003373.pdf>
- Observatorio de la Seguridad de la Información [INTECO]. (2012). *Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA)*. INTECO. <https://www.aguasresiduales.info/revista/libros/estudio-sobre-la-seguridad-de-los-sistemas-de-monitorizacion-y-control-de-procesos-e-infraestructuras-scada>
- Okta. (2023). Okta Identity Cloud. <https://www.okta.com>
- Organization of American States [OAS]. (2017). Why a cyber-risk oversight? En *Cyber-Risk oversight handbook for corporate boards* (p. 4). OEA. <https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf>

- Palo Alto Networks. (2023). Next-Generation Firewalls. <https://www.paloaltonetworks.com/>
- Patiño Mazo, E. (2018). Planeación estratégica de mercadeo y relaciones de transferencia en el ecosistema digital. *Espacios*, 39(50), 13-27. <https://www.revistaespacios.com/a18v39n50/a18v39n50p13.pdf>
- Pérez Zúñiga, R., Mercado Lozano, P., Martínez García, M., Mena Hernández, E., & Partida Ibarra, J. A. (2018). La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, 8(16), 847-70. https://www.scielo.org.mx/scielo.php?pid=S2007-74672018000100847&script=sci_arttext
- Rosales Montalbán, E. A., Martelo Gómez, R. J., & Franco Borré, D. A. (2020). Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit. *Aglala*, 11(1), 227-245. <https://revistas.uninunez.edu.co/index.php/aglala/article/view/1579>
- Sain, G. (2018). La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas. En *Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet* (pp. 7-32). Erreius. <https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf>
- Sáinz Peña, R. M. (2016). Ciberseguridad, la protección de la información en un mundo digital. *Revista TELOS*. <https://n9.cl/n5bry>
- Sánchez Holguín, A. del M., Imán Sánchez, A. N. K., Chocan Sosa, E. A., Barreto Espinoza, K. L., & Torres Ruiz, M. I. (2023). *Propuesta de mejora de los servicios del taller R&T a través de un análisis de procesos aplicando metodologías de mejora continua* [Final project, Universidad de Piura]. Repositorio UDEP. <https://pirhua.udep.edu.pe/backend/api/core/bitstreams/b2a30486-9b67-46dc-b341-3499a699d2d3/content>
- Schmitt, U. (2018). Rationalizing a personalized conceptualization for the digital transition and sustainability of knowledge management using the SVIDT Method. *Sustainability*, 10(3), 839. <https://doi.org/10.3390/su10030839>
- Sepúlveda Marcial, C. M., & Medina Ulloa, O. L. (2024). *Desarrollo de un sistema tutorial inteligente para la implementación del modelo de medición de madurez y territorios inteligentes para Colombia (MMMCTIC)* [Bachelor's thesis, Universidad Santo Tomás]. <https://n9.cl/4udig>
- Teslia, I., Yehorchenkov, N., Iegorchenkov, O., Kataieva, Y. (2016). Enterprise information planning - A new class of systems in information technologies of higher educational institutions of Ukraine. *Eastern-European Journal of Enterprise Technologies*, 4(2), 11-23. <https://journals.uran.ua/eejet/article/view/74857>
- Valencia Duque, F. J. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000*. Universidad Nacional de Colombia. <https://repositorio.unal.edu.co/bitstream/handle/unal/80158/9789587946017.pdf?sequence=2&isAllowed=y>
- Vial, Gregory. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, 28(2), 118-44. <https://n9.cl/3rlun>
- World Economic Forum. (2013). *Global Risks 2013* (8th ed.). World Economic Forum. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

Chapter 2

Blockchain and Cybersecurity: Building Digital Trust^{*}

DOI: <https://doi.org/10.25062/9786287818064.02>

Jaider Ospina Navas

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: This chapter explores the cutting-edge developments in blockchain technology to identify its role in creating a secure digital ecosystem. To achieve this, it outlines the key characteristics of blockchain, including decentralization, immutability, and consensus; discusses its benefits regarding security, transparency, and resistance to tampering; examines the various types of attacks on immutability that are recognized to date; describes the different applications of blockchain; and presents the current challenges and limitations, offering a comprehensive view of the possibilities and obstacles in this evolving field.

Keywords: blockchain; digital trust; decentralization; digital ecosystem; immutability; transparency

* 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

Jaider Ospina Navas

PhD student in Information Systems. Master's in Information and Communications Sciences and Bachelor of Electronic Engineering, Universidad Distrital Francisco José de Caldas, Colombia. Cybersecurity consultant and cloud solutions architect.

<https://orcid.org/0000-3251-3017> - Contacto: jaider.ospina@esdeg.edu.co

APA Citation: Ospina Navas, J. (2025). Blockchain and Cybersecurity: Building Digital Trust. In M. E. Realpe Díaz & A. M. González González (Eds.), *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* (pp. 43-68). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818064.02>

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

This chapter explores the state of the art of blockchain technology to identify its role in building a secure digital ecosystem. The general objective is to specify the characteristics that allow for creating a reliable digital ecosystem through enabling agents that guarantee data privacy, confidentiality, and availability, as well as to provide a view of the main limitations of its adoption. For this, we review articles that evaluate aspects of cybersecurity, documentation of applications or initiatives to improve digital trust, and studies in which a systematic literature review is carried out.

Birth of Blockchains

Although the origin of the blockchain (BC) is associated with the publication of the whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System,” it should actually be attributed to the work of Stuart Haber and W. Scott Stornetta. In their article “How to Time-Stamp a Digital Document,” published in the *Journal of Cryptology* in 1991, they introduced a digital time-stamp system to certify the date of creation or modification of an electronic document, without depending on the physical medium, using cryptographic hashes to generate unique summaries of documents and store them in a blockchain (Haber & Scott, 1991).

Subsequently, on November 1, 2008, Satoshi Nakamoto, a pseudonym used by the person or group that created the concept and underlying technology of Bitcoin, sent a message to the cryptography mailing list metzdowd, announcing a new electronic money system based on peer-to-peer (P2P) networks. This document laid the theoretical and technical foundations of blockchain technology

and concisely explained the technical aspects proposed by a new digital currency, as well as the main objective of its creation: to dispense with trusted third parties.

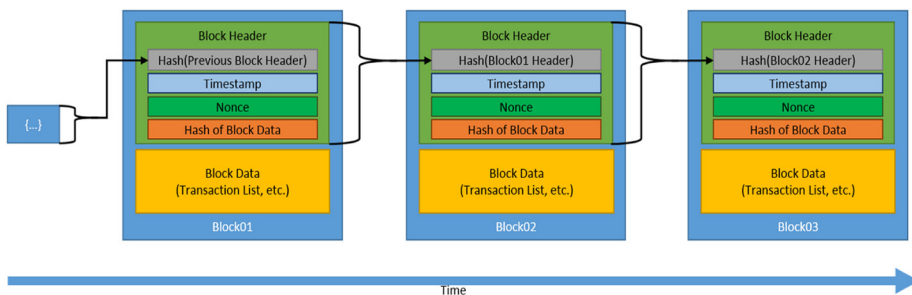
“What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party” (Nakamoto, 2008, p. 1).

Thus, the most recognized digital currency, Bitcoin, was born, and a solution is proposed for one of the biggest problems of this type of currency: double-spending. By using a decentralized blockchain and a distributed consensus to validate and record transactions securely and transparently, different systems and applications inherit characteristics to protect data and create a reliable digital ecosystem.

Fundamentals of Blockchain Technology

Blockchain is a distributed and secure database that has revolutionized data storage and verification (Xu et al., 2019). Each block in the chain contains a cryptographic hash of the previous block intertwined by a hash guaranteeing a “digital signature”¹ for its integrity and eventual manipulation, a timestamp, and data of the transaction made (Figure 1).

Figure 1. *Generic Blockchain*



Source: NISTIR 8202 (2018).

Generally, BC can be conceived as a decentralized and secure data logging technology, which has emerged as a fundamental component in the digital era. According to Nakamoto (2008), blockchain is defined as a “public transaction ledger” that stores information immutably and transparently. The strength of BC lies in its decentralized nature, where multiple network nodes verify and validate

transactions, eliminating the need for a central trusted intermediary (Swan, 2015). This guarantees the security and integrity of the stored data since any attempted alteration would require the consensus of the majority of participants, making it highly resistant to tampering and cyberattacks (Krichen et al., 2022; Mougayar, 2016; Yli-Huumo et al., 2016). As already mentioned, BC's unique structure makes it resistant to tampering, as any change to one block would require changes to all subsequent blocks to maintain chain coherence (Popchev et al., 2021).

Speaking specifically of the Bitcoin protocol described initially by Nakamoto, it is based on the TCP/IP protocol stack from which a network of nodes is built overlaid on the internet. The nodes make up a P2P network where all nodes provide and consume services simultaneously while collaborating via consensus services Vamsi_Cz5cgo and Vamsi_Cz5cgo (2020).

Blockchain and Distributed Ledger Technology

Distributed Ledger Technology (DLT)

Strictly speaking, BC is a specific type of DLT, and, in turn, DLT is a particular case of distributed database characterized by its consensual validation process (Romero, 2018). DLT is characterized by three articulated technological elements to make up its architecture: P2P networks, asymmetric cryptography, and consensus algorithms. A significant difference between DLT and BC lies in their structure and operation. While DLT can have different degrees of decentralization and can be public or private, BC is entirely decentralized and generally public (Hurtado, 2021). Examples of DLT platforms are Hyperledger Fabric, Corda, and Quorum, which are some of the most representative ones. These technologies can be public or private and customized to adapt to the specific needs of an application or industry.

Types of Blockchains

There are several types of BC, each with its characteristics and capabilities that adapt to different needs.

Public Blockchains

Networks that anyone can join to verify transactions and participate in block validation. Users are generally anonymous, and no participant has more rights than

the others, so there are no network administrators. They are considered drivers of distributed ledger technologies (DLT) and P2P networks for data distribution (Haleem et al., 2021). The most well-known public networks are Bitcoin, Bitcoin Cash, Ethereum, and Litecoin.

Private Blockchains

Networks where access is restricted to a specific group of entities. They are commonly used by companies that want to take advantage of BC technology but maintain control over who can participate in the network and all management tasks, such as creating and accepting blocks.

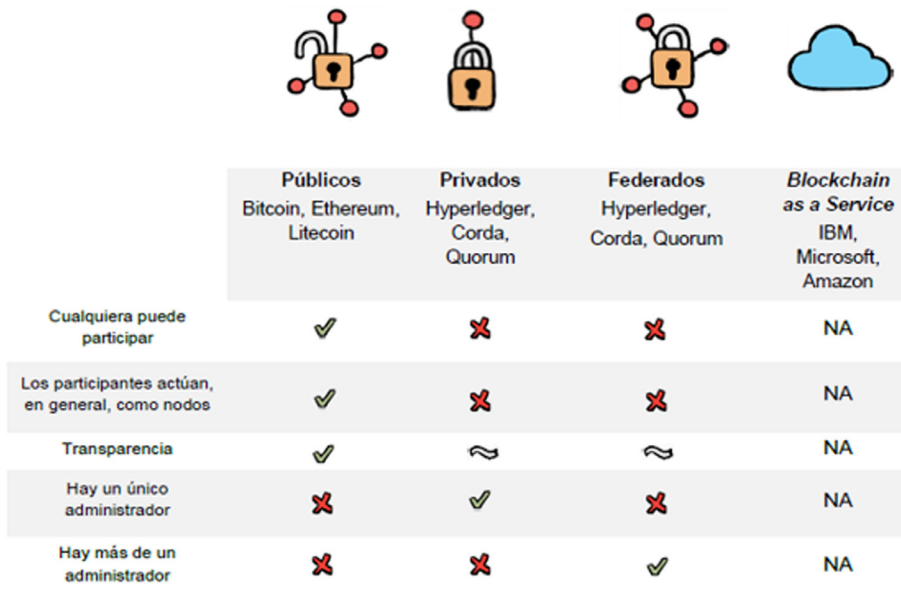
Federated or Consortium Blockchains

A hybrid implementation of the previous types. Control does not rest with a single entity but with a group, allowing a certain level of privacy to be maintained while taking advantage of the security and transparency of BC technology.

Blockchain as a Service (BaaS)

Products enabling users to build their networks and concentrate on developing applications without concern for the underlying infrastructure and the technical aspects. Figure 2 shows some particularities of the different types of BCs.

Figure 2. Types of Blockchain Networks



No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart Contracts	✓	✓	✓	NA
Existe recompensa por minado de bloques	≈	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	≈	NA
Seguridad basada en protocolos de consenso	✓	✗	≈	NA
Seguridad basada en funciones hash	✓	≈	≈	NA
Provee servicios en la nube	NA	NA	NA	✓

✓ Sí ✗ No ≈ A veces NA No Aplica

Source: López (2018).

Blockchain Generations

In the article “Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption Using BloT for Smart Government and Industry 4.0,” Hasan et al. (2022) identify five generations of BC since its appearance: 1st generation: It focuses on the creation of bitcoin by Satoshi Nakamoto in 2008, a decentralized digital currency that allows P2P transactions without an intermediary; 2nd generation: It introduces the idea of Smart Contracts, programs that run automatically when certain conditions are met. Ethereum is the best-known example; 3rd generation: It revolves around solving scalability and interoperability issues faced by previous generations. Projects like Cardano and Polkadot are working on solutions to allow different BCs to interact and handle a higher number of transactions, going from six transactions per second (TPS) to 100,000 TPS. This generation introduced decentralized applications (dApps); 4th generation: It deals with integrating existing business and government systems, providing solutions for interoperability, privacy, and security issues (Banafa, 2022). A level of 300,000 TPS has already been reached, and the range of applications increases in fields such as the supply chain, electronic voting, and Smart Grid; and 5th generation: It is the current one and is in the process of gestation, which according to experts, emerges with projects such as Relictum

Pro (Bitcoin.es, 2020). It is characterized by the use of intelligent machines and data analytics to automate smart application processes (Choi & Siqin, 2022).

Distinctive Features of Blockchain Technology

Some characteristics of BC that have become potentiating elements of cybersecurity strategies are decentralization, immutability, transparency, and consensus. These pillars have transformed reliability and security in online operations, and understanding them is essential to appreciate the potential of this technology.

Decentralization

According to Tapscott and Tapscott (2016), decentralization means no central authority controls the network. Instead of relying on a centralized entity like a bank or government, transactions are verified and recorded on a distributed network of collaborative nodes. Eliminating intermediaries builds trust and reduces single points of failure, making the network highly resistant to censorship and eventual attacks that compromise data. Decentralization has several advantages:

- Provides a trustless environment: In a decentralized BC network, no one has to know or trust anyone else. Each member holds an exact copy of the same data in a distributed ledger.
- Improves data reconciliation: All nodes can access a shared, real-time data view.
- Reduces points of weakness: Decentralization can reduce points of weakness in systems that depend on specific actors. A point of weakness may be due to a dependency on specific resources such as storage or computing capacity.
- Optimizes resource distribution: Optimized resource distribution enhances network performance and consistency through strategies such as improving content delivery times.

Immutability

According to Mougayar (2016), immutability is a principle that refers to the inability to change or delete once a transaction has been recorded on the blockchain. Each block of data in the chain is cryptographically linked to the previous one, making it extremely difficult, if possible, to modify the contents of one block without altering

all of the following. This ensures that recorded transactions are permanent and reliable, essential in applications where data integrity is crucial, such as healthcare and identity management.

Transparency

In a BC network, all transactions are visible to all network participants, providing high transparency. However, this transparency can pose challenges, especially when sensitive data is involved.

According to Sedlmeir et al. (2022), transparency presents challenges to companies and the public sector related to an excessive degree of it. They point out how the types of sensitive data involved in different blockchain use case patterns and argue that the implications of BC information exposure caused by the storage and execution of replicated transactions go beyond the conflict often mentioned with the “right to be forgotten” of the GDPR and may be more problematic than anticipated. The authors describe the balance between protecting sensitive information and increasing process efficiency through smart contracts. They also explore the extent to which permissioned blockchains and new applications of cryptographic technologies, such as autonomous identities and zero-knowledge proof, can help overcome the challenge of transparency and, therefore, act as catalysts for the adoption and dissemination of BC in organizations.

As mentioned, one proposal to attack this problem is through zero-knowledge proof (ZKP). This cryptographic technique can be used in the blockchain environment to verify if the prover has a sufficient number of transactions without leaking private transaction data (Konkin & Zapechnikov, 2023).

Similarly, Sun et al. (2021) conducted a study on ZKP in the blockchain environment to highlight security issues and challenges and discuss the framework, models, and applications of ZKP. In conclusion, ZKP is a valuable tool for improving privacy and security in blockchain transactions, allowing transactions to be verified without revealing sensitive details.

Consensus

Consensus is achieved through algorithms, thanks to which the “network makes consensual decisions, validates the information, and assigns tasks to each of the nodes comprising it” (Criptodemy, n.d.). This concept was initially introduced by Adam Back in May 1997 and sought to regulate the excessive abuse of internet resources, such as emails and anonymous remailers (Back, 2002).

In the words of Narayanan et al. (2016), consensus can be defined as a process by which nodes agree on the validity of a transaction before adding it to the blockchain. The most significant example of this type of consensus protocol can be found in the proof of work (PoW) used by Bitcoin. This protocol involves miners competing to solve complex mathematical problems, and the first to do so has the right to add a new block. This mechanism ensures that all parties in the network agree on the status of the blockchain and that transactions are valid and secure.

Consensus Algorithms

There are various consensus protocols and algorithms to ensure network security and reliability; each one defines its characteristics and advantages. Some are:

Proof of Work (PoW)

PoW is the most well-known consensus protocol, primarily associated with Bitcoin and Ethereum, although it is used in other cryptocurrencies and blockchain networks. In essence, proof of work requires network nodes to perform computationally intensive calculations to demonstrate that they have invested time and resources into verifying transactions. This process is known as *mining*, and the participants are called *miners*. It is continually repeated to keep the blockchain secure and distributed.

According to Narayanan et al. (2016), proof of work is a complex mathematical puzzle requiring a large amount of computing power to solve. Miners compete to solve this puzzle, and the first to do so has the right to add a new block to the chain and is rewarded with new coins (e.g., bitcoins) and transaction fees.

Nakamoto (2008) first introduced the concept of *proof of work* in the context of Bitcoin and provided the theoretical foundations for its operation. In Nakamoto's own words, its adoption is similar to that presented by Back (2006), Hashcash. This algorithm was initially used to address email spam and DDoS attacks and is currently used for transaction verification purposes.

PoW, as a consensus protocol, has proven effective in preventing malicious attacks and creating a secure and reliable record of transactions on the blockchain network. However, its greatest weakness is its poor scaling capacity and limited performance in terms of transactions per second (TPS). This protocol is perhaps one of Nakamoto's most outstanding contributions to the creation of BC. At the

same time, it has solved one of the most challenging problems in computing, known as the Byzantine generals problem. Advantages: proven security, high attack resistance of 51%. Disadvantages: high energy consumption, centralization in mining.

Proof of Stake (PoS)

In PoS, validators lock a certain amount of cryptocurrency as collateral, and the probability of being selected to validate a block is based on the number of coins at stake. Ethereum has migrated PoS with Ethereum 2.0. This type of consensus was introduced as a more efficient and less expensive alternative to (PoW). Instead of requiring miners to perform intense computational calculations, PoS allows network participants to create blocks and validate transactions based on the number of coins they own and are willing to “stake” for consensus (Ge et al., 2022).

There is a wide variety of consensus algorithms derived from PoS, including, but not limited to, DPoS, Snow White, Sleepy Consensus, Ouroboros, Ouroboros Praos, Ouroboros Genesis, Ouroboros Cryptsinous, EOS, Improvement of DPoS (Ge et al., 2022).

Advantages: energy efficiency, less centralization, incentivizes coin holders, fewer barriers to entry (the network accepts participants without the need to purchase and configure expensive hardware), faster transactions compared to PoW networks. Disadvantages: possible centralization based on wealth, as those with more coins have more opportunities to create blocks; the “nothing at stake” problem; there is no actual cost associated with validating incorrect blocks, which can lead to security issues.

Delegated Proof of Stake (DPoS)

This is a variant of PoS in which a community-chosen group of validators is responsible for validating transactions. EOS is an example of a blockchain that uses DPoS. Advantages: high scalability and speed in confirming transactions. Disadvantages: less decentralization and power concentration in the chosen nodes.

Proof of Authority (PoA)

Algorithms are based on reputation, where validators do not risk cryptocurrencies but their reputation; consequently, they are chosen arbitrarily as they are considered trustworthy. Its use primarily occurs in private networks, including

logistics, where it is seen as an efficient and sensible solution because its nature enables the harnessing of the characteristics of BC while preserving participants' privacy. Advantages: energy efficiency, high speed compared to PoW and PoS, monetary incentives. Disadvantages: less decentralization since it is based on a limited number of block validators; vulnerable to collusion, as a limited number of validators are trusted, with the risk that they may collude to act maliciously.

Proof of Space and Time (PoST)

This is a new cryptographic primitive that allows a prover to convince a verifier that they have spent a "space-time" resource. In the words of Ortega (2023), "... in the Proof of Space and Time algorithm, network nodes must demonstrate that they are storing a specific amount of data through a process called farming." Advantages: energy efficiency, which may be possible to mine with this algorithm on standard devices; accessible to more participants; decentralization of the process. Disadvantages: permanent growth because as more miners are added to the network, more storage space is required (Moran & Orlov, 2019).

Round Robin

Round Robin in BC has been studied in several scientific papers. A proposal for its use is presented by Raikwar and Gligoroski (2021), who propose the R3V consensus protocol. This selects a set of leader candidates rotating based on seniority. They then compete to be the leader of the block by solving a puzzle based on a verifiable delay function (VDF) (Raikwar & Gligoroski, 2021). Advantages: greater resistance against most attacks common in PoS protocols, lower power consumption, less communication complexity, and greater fairness. Lastly, other existing less widespread algorithms are proof of weight (PoW), proof of importance (PoI), proof of coverage (PoC), and directed acyclic graphs (DAG).

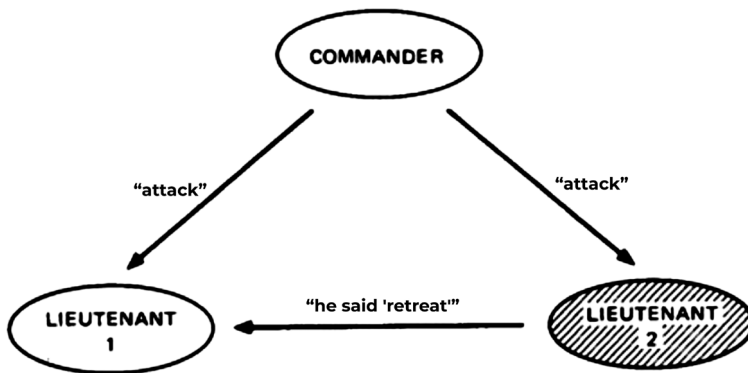
The Byzantine Generals Problem: A Military Perspective

The Byzantine generals problem was stated by Robert Shostak and developed with Leslie Lamport and Marshall Pease in 1982 at the scientific and technological research center SRI International (BBC News Mundo, 2020). It undoubtedly captures the essence of the problem of consensus in a network with untrustworthy agents.

From a game theory perspective, it describes the extent to which decentralized parties experience difficulties in reaching consensus without a trusted central agent.

In essence, a war scenario is proposed where a group of Byzantine generals besieges a city from various points, and it must be agreed whether to attack or retreat in a coordinated manner. Only one general can give the order to the entire force since he is the commander. The rest of the generals are considered lieutenants. Lieutenants communicate with each other when they receive orders from the commander, and the two possible orders from the commander are "attack" and "retreat." It is known that one or more generals can be traitors. The goal is for all loyal generals NOT to agree. To do this, they may provide incorrect information. For example, if the commander is a traitor, he may send conflicting orders to different lieutenants. If the lieutenant is a traitor, he can show it to the other lieutenants to confuse them and make them believe that the traitor is the commander and that the commander sent them orders contrary to his orders (Soto, 2020). A successful battlefield solution must lead to one of two outcomes: 1) all loyal lieutenants make the same decision, and 2) if the commander is loyal, all lieutenants will faithfully carry out his orders. Figure 3 illustrates the case where "Lieutenant 2" is a traitor.

Figure 3. *Lieutenant 2 Is a Traitor*



Source: Lamport et al. (1982).

These problems are associated with the need for consensus and the possibility of unreliable actors in the system. A reliable computer system must deal with malfunctioning components that provide conflicting information to various system parts. The problem is finding an algorithm that guarantees loyal generals reach an

agreement. It was shown that using only verbal messages could solve this problem if more than two-thirds (2/3) of the generals were loyal. A traitor can confuse two loyal generals. This problem is transferred to the blockchain world when it is necessary to add a new block to the chain, where each node must agree on the status of the system before becoming part of it. Clearly, in our context, "loyalty" is a constitutive aspect of trust.

Threats in a Blockchain Network

The most outstanding aspect of building a secure system that BC offers is its immutability. However, this is not 100 % guaranteed to be invulnerable. BC can be compromised under certain circumstances. Some of these possible scenarios are:

- 51 % attack: This type of attack is caused by the possibility that a group of miners controls more than 50 % of the network's computing power, thereby being able to change and reorganize the blockchain (affecting its integrity), override previous transactions, and create an alternative chain. However, performing a 51 % attack on a network with many miners is highly costly, although such attacks have been identified (Sayeed & Marco-Gisbert, 2019).
- Sybil attack: It is named after the book *Sybil* (Schreiber, 1973) and the story of a woman diagnosed with dissociative disorder. The attack is characterized by P2P networks corrupted through the creation of false identities. The vulnerability of a BC network to this attack will depend on the cost of generating identities, the degree to which the reputation system accepts new identities, and whether the reputation system treats all entities identically. Mohaisen and Kim (2013) identify three main defense strategies: 1) trusted certification entities, 2) resources testing (IP testing, network coordinates, and algorithm resolution, among others), and 3) social networks (Mohaisen and Kim, 2013).
- Double-spending attacks: Although most blockchains are designed to prevent double-spending, in certain circumstances, an attacker could attempt to spend the same cryptocurrency twice before the network updates its status. This risk occurs in chains with slow transaction confirmations. There are different types of double-spending attacks. A recent study presents an attack called Adaptive Double-Spending Attack (Adaptive DSA) as an advanced double-spending attack in PoW-based BCs.

The attacker duplicates a valid transaction in the network and converts it into a Markov decision process (MDP), and through focused exploitation in stochastic dynamic programming (SDP), optimized Adaptive DSA attack strategies are exploited (Zheng et al., 2023).

- Presence of protocol vulnerabilities: Bugs or vulnerabilities in a blockchain's software or protocol can be exploited to compromise immutability. For instance, errors in the code implementation can allow an attacker to make invalid transactions or alter the status of the chain.
- Forks and protocol upgrades: Sometimes, a blockchain may experience a fork or protocol upgrade that could affect immutability. If a community disagrees with changes to the protocol, it could result in two separate chains (hard forks), which could have implications for the immutability and continuity of the chain.

Blockchain, Disruptive Technology

BC technology is one of the greatest innovations of the 21st century, with a significant impact on sectors such as finance, manufacturing, electronic voting, and education, to name a few. This section includes systematic reviews conducted by third parties that assess the impact of BC on various areas. The aim is to validate the hypothesis that implementing blockchain technology can significantly enhance digital trust by providing a decentralized and transparent system. This guarantees data integrity and immutability, which could lead to greater adoption of digital services, a reduction in fraud, and improved efficiency of digital transactions.

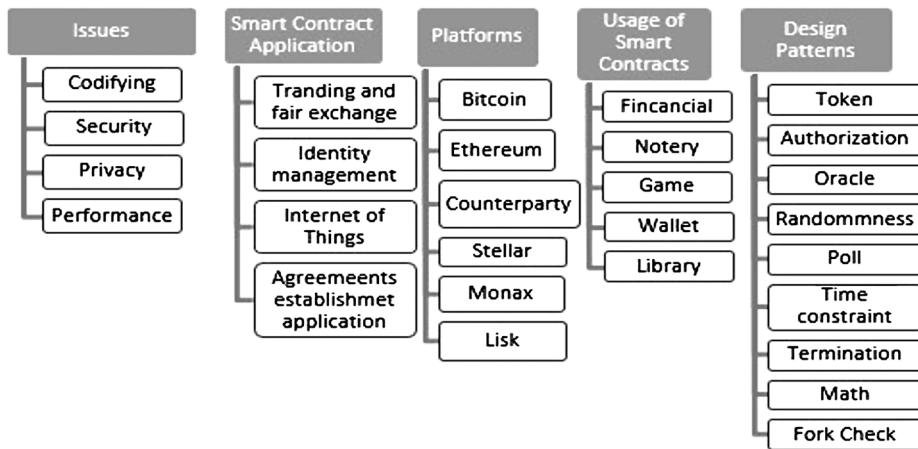
Works such as Baena and García's (2022) establish, after a rigorous bibliographic review, a consensus regarding the benefits of security, transparency, traceability, trust, authenticity, privacy, and the reduction of costs in supply chains through blockchains.

For their part, Xu et al. (2019) studied 756 articles, which were narrowed down to 119 under the economics and business criteria. They highlight the potential impact in areas such as crowdfunding and accounting management, data storage and sharing, supply chain management, and smart trading to benefit from BC characteristics (Xu et al., 2019).

Leka et al.'s study examines 292 papers extracted from databases such as IEEE, ACM, Science Direct, and Springer, focusing its final diagnosis on 28 papers regarding the use of blockchain (BC) in smart contracts. It identifies code

errors, malicious attacks, and exploitations of miners and users as the principal vulnerabilities. Additionally, it reviews various tools and methods for verifying and auditing smart contracts. Figure 4 presents an interesting classification diagram that includes aspects such as coding, security, privacy, and performance, all of which are relevant to any application and field where BC is used. Therefore, it is advisable to adopt its taxonomic approach when evaluating particular use cases (Leka et al., 2019).

Figure 4. Smart Contract Classification Diagram



Source: Leka et al. (2019).

Romero (2018) highlights the use of distributed ledger technology (DLT) in financial transactions, with advantages such as accelerating the settlement process of financial transactions, reducing the number of intermediaries, and improving the efficiency of the reconciliation process. He shows how it can enhance the transparency and traceability of transactions, which is especially useful in international trade, where there are many actors, and facilitates the negotiation and post-negotiation of securities, regulatory compliance, and digital identity management. Besides, the trend toward a total digitalization of the economy is clear. Aspects such as the digital transformation based on the Fourth Industrial Revolution have led to an economy considered digital (Bogdanov et al., 2021), where BC is used as a technological enabling element.

At this point, it is evident that the impact of BC has expanded beyond its use in cryptocurrencies. BC has become a mainstay in various fields such as supply chain, healthcare, and intellectual property protection. According to Tapscott and

Tapscott (2016), blockchain provides greater visibility and traceability in the supply chain, allowing for real-time tracking of products from origin to destination. In the healthcare sector, Griggs et al. (2018) point out that blockchain guarantees the security and privacy of electronic medical records, facilitating the secure exchange of information between doctors and patients. Furthermore, blockchain offers an immutable record of authorship and ownership of digital content in copyright and intellectual property, which can be fundamental for protecting creators' rights (Lorenzo, 2020).

All-in-all, BC can help improve trust and collaboration among different parties in sectors such as Industry 4.0. Haleem et al. (2012, 2022) highlight several enabling aspects of BC in smart cities, smart factories, smart products, and supply chains.

Regarding social responsibility, the proposal to use BC as an audit instrument and operating model is interesting (Martínez et al., 2020), thanks to the data logging model that can be employed in wallets.

Authors such as Haleem et al. (2021) identify a wide range of BC applications and features, such as distributed accounting that enables secure and audited transmission of patient medical records and drug supply chain management. However, the main obstacle is the lack of experience in the field of applications that use BC technology. Another example of the use of BC is the drug supply chain (Casino et al., 2019).

On the other hand, architectural scenarios in which BC is used as a solution to problems in the centralization of resources in IoT networks enable the storage of sensor data centrally instead on the distributed basis of BC, where sensor data can be managed similarly to the blockchain philosophy (Conoscenti et al., 2017).

Blockchain and Cybersecurity

While some characteristics that make BC a dynamic agent of cybersecurity have already been mentioned, some aspects that they reinforce are:

Advantages and Benefits

- Greater security and data protection due to its immutable structure
- Improved data transparency and integrity through distributed auditing and verification
- Highly available and resilient architectures

- Reduced points of vulnerability and risk through decentralization and resistance to cyberattacks

Practical Applications of Blockchain in Cybersecurity

- Identity protection and authentication through IDMS (identity management systems) systems to manage authentication, authorization, and file sharing
- Logging and verification of security events for intrusion detection and forensic analysis
- Data access and control management through smart contracts
- Distributed accounting and operational transparency
- Redundant and resilient architectures

Challenges and Considerations Regarding the Use of Blockchain in Cybersecurity

- Scalability and performance
- Privacy and protection of personal data in transparent BC environments
- Update and maintenance of BC infrastructure to ensure long-term security
- Collaboration and development of BC standards focused on cybersecurity
- Cooperation among the actors involved, such as developers, researchers, and end-users
- Statement of good practices for BC implementation in cybersecure environments

Building a Digital Trust Ecosystem

There are numerous and diverse fields of use of blockchain technology and its potential for building digital trust. But this, like all technology, is not a panacea. Its adoption is a process that must be built daily and with the participation of all stakeholders and, above all, guarantee its use as a means and not as an end. A priori, BC conceives security by design based on immutability, integrity, and transparency characteristics. Once transactions are confirmed, the data is permanently stored in the tamper-proof ledger, and these transactions are safeguarded. In terms of design, BC technology includes cryptography and distributed consensus as

preventive mechanisms to reduce cyberattack risks and a distributed architecture without requirements for central “trusted” entities. Without trusted intermediaries, trust within a BC network is made possible by four key features: 1) ledger: It provides transactional traceability. Unlike traditional databases, transactions in BC are not deleted; 2) security: Data is considered cryptographically secure, guaranteeing non-tampering; 3) sharing: The ledger is shared among several participants, which provides transparency; and 4) distributed nature: It allows the number of nodes in a BC network to be scaled to make it more resistant to possible cyberattacks and optimize the delivery and consumption of content.

Thus, the key pillars of information security (immutability-integrity, availability-distributed and redundant networks, transparency-distributed audit), combined with the construction and adoption of practices and strategies in cybersecurity, ultimately allow us to build a reliable digital ecosystem.

At the national level, it is worth highlighting that the Ministry of Information and Communications Technologies expressly states the potential for building digital trust:

The key of DLT/Blockchain is to build “trust” in the transactions carried out on the network, to the point that neither physical documents (papers) nor centralized entities (banks or notaries) are required to possess a security that represents social or economic value. (MinTIC, 2022)

In the national context, it is important to highlight the integration between the government and the Inter-American Development Bank (IDB) to promote BC through initiatives such as the space for experimenting with BC projects in the public sector, which was born from the signing of a memorandum of understanding with IDB Lab, the IDB’s innovation laboratory.

Likewise, the MinTIC published the “Reference Guide for the Adoption and Implementation of Projects with Blockchain Technology for the Colombian State.” This facilitates the State’s approach to this technology, promotes an ethical and compliance approach, introduces a governance approach, presents guidelines for developing projects in government agencies, and provides tools so that projects are designed and operated in an organized, staggered, and structured manner.

Discussion

Conversely, the promise of BC as a high-impact technology in different fields and its potential to ensure cybersecurity practices must be responsibly addressed.

Problems such as the limitation in scalability derived from the size that BC can reach would be solved by implementing chain pruning algorithms, which implies that "old transactions could be eliminated, saving only their hash, to preserve the integrity of the chain" (Pérez & Joancomartí, 2014).

The challenges BC faces in decentralized environments can be overcome using network protocols such as Named Data Networking (NDN). This can contribute to driving BC by enhancing effective content delivery through name-based routing and caching in the network. This approach allows for efficient content delivery and improved data transfer, particularly in decentralized networks where efficiency is crucial (Guo et al., 2019; Kharjana et al., 2023). However, it is worth clarifying that NDN is not directly compatible with BC since BC applications (without permissions) generally require the transmission of transactions and blocks in real time, which is not compatible with the "pull" design of NDN.

Under this premise, BoNDN (BC over NDN) becomes an integration alternative. This is based on a core NDN design and processes each type of data that needs to be transmitted individually (Guo et al., 2019). BoNDN proposes a push-subscription approach to support block transmission, in which each miner makes a subscription. Once a block is generated, the subscribed miner will receive the block (Benmoussa et al., 2023).

In the field of application development, the emergence of architectural patterns specific to BC is already a reality that heralds the evolution of the technology in question. Alzhrani et al. (2023) describe twelve patterns applicable to 400 existing applications.

Along these lines is the development of Byzantine fault-tolerant (BFT) algorithms and libraries. Castro and Liskov (2001) describe a new BFT replication algorithm developed to design highly available systems that tolerate Byzantine faults. The algorithm is used in asynchronous environments such as the internet, and it incorporates mechanisms that prevent faulty nodes and allow for proactively rapid recovery of replicas. Its fault tolerance is guaranteed if less than 1/3 of the replicas fail in the failure window. Castro and Liskov (2001) also present an implementation of the algorithm as a generic library and its application to build the first Byzantine fault-tolerant NFS file system.

Having said that, authentication alternatives other than traditional ones, such as attribute-based encryption (ABE), guarantee that only those with specific attributes can access information, which can be an effective solution for access control and encrypted data sharing (Hong et al., 2022). ABE can generally be

divided into two patterns: ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). The access policy is incorporated into the ciphertexts, and the user's private key is associated with a collection of attributes such as location, age range, email addresses, etc. However, ABE can be vulnerable to attacks such as key abuse and custody (Arshad et al., 2023). In summary, ABE is a powerful tool for access control and data sharing, but it presents challenges that must be addressed for effective implementation.

In terms of trust, so-called permissionless BC networks provide trust capabilities among parties without prior knowledge of each other. This principle can allow transactions to be carried out directly, delivering transactions faster and at lower costs. On the other hand, a BC network that more strictly controls access, called a permissioned network, where there is a certain level of trust among the parties, has capabilities that help reinforce that trust.

Another fundamental aspect is the performance that results from the high relevance to allow for the evolution of technology; this is promising given the increase in transactions per second (TPS), going from 4–6 TPS in the first generation BC to 100,000–300,000 TPS in the fourth and the potential that will be unlocked in a fifth generation with the adoption of technologies such as 6G (Hasan et al., 2022).

The availability of BC networks could not be left out of this discernment. Permanently interacting with cyberspace has created a strong dependence on applications and interaction spaces that constitute a "vital" ecosystem. In this context, the construction of high resource availability is decisive, guaranteeing a service without failures and interruptions (Castro & Liskov, 2001).

It is well known that the first strategy in availability is replication. Thanks to this, redundancy is achieved by providing resources that may eventually fail and "taking over" redundant resources. In BC, replication and fault-tolerant algorithms such as BFT (Byzantine-fault-tolerant) help build hierarchical structures that optimize the use of resources and increase scalability (Rahulamathavan et al., 2017).

The latter may be undesirable in devices with low storage capacity, which shows that BC must be able to adapt to different scenarios, knowing how to "exploit" particular features for specific needs. So, the advantage that total and cumulative data protection on the blockchain may represent might not be desirable in other scenarios.

Blockchain storage is carried out with great redundancy: Every full node in the network contains an entire copy of the BC (and its transactions), allowing these nodes to validate each new transaction correctly. However, maintaining a complete

copy of the chain can be a problem for nodes that operate on lightweight devices such as mobile devices (Pérez & Joancomartí, 2014).

Finally, it is worth reflecting on whether BC is “magic” capable of solving all modern problems, as suggested by many articles, and as Clarke (1962) stated in his third “law”: “Any sufficiently advanced technology is indistinguishable from magic.” The answer is no. This must be considered alongside the development of an information security culture, after evaluating its engineering implications in the field of exploration.

Conclusions

Blockchain introduces disruptive aspects in constructing information systems and applications that preserve immutability and transaction records. Concepts such as decentralization, immutability, and consensus are fundamental in BC and have revolutionized how we handle and trust digital data. Decentralization eliminates the need for intermediaries; Immutability ensures data integrity, and consensus ensures that all parties reach reliable agreements in a distributed network. These principles are the foundation of security and trust in BC-based applications and can potentially transform numerous industries.

Although transparency is one of the main advantages of blockchain technology, it can also pose challenges, especially when protecting sensitive data and complying with privacy regulations. Aspects like this, along with high energy consumption and growth in node size, can limit the adaptation of BC as a technology. However, several strategies have been documented in this work to overcome it.

Thus, combinations such as using NDN and BoNDN to address connectivity problems with the immutable and reliable distributed ledger feature of BC can guarantee that the data exchanged is trustworthy and less susceptible to packet losses and cyberattacks.

Blockchain is not a solution on its own. It is a technological tool that must be accompanied by a strategic plan that understands the project's needs, identifies the degree of transparency and decentralization, determines the members who will act as nodes, and establishes the appropriate blockchain structure, defining the transactions or smart contracts to be executed (MinTIC, 2020).

This critical review includes aspects of the different considerations for developing solutions that, through BC, ensure cybersecurity and, thus, build a reliable digital ecosystem.

References

- Ali, R., Clarke, D., & McCorry, P. (2017). Towards developing a blockchain-based approach for the secure storage of patient records. In *IEEE International Conference on E-Health Networking, Applications and Services* (pp. 400-406). IEEE.
- Alzhrani, F., Saeedi, K., & Zhao, L. (2023). Architectural patterns for blockchain systems and application design. *Applied Sciences*, 13(20), 11533. <https://doi.org/10.3390/app132011533>
- Amazon Web Services. (n.d.). What is decentralization? <https://aws.amazon.com/es/blockchain/decentralization-in-blockchain/>
- Arshad, H., Picazo-Sanchez, P., Johansen, C., & Schneider, G. (2023). Attribute-based encryption with enforceable obligations. *Journal of Cryptographic Engineering*, (13), 343-371. <https://doi.org/10.1007/s13389-023-00317-1>
- Back, A. (2002). Hashcash - A denial of service counter-measure [Technical report]. <http://www.hashcash.org/papers/hashcash.pdf>
- Baena-Luna, P., & García-Río, E. (2022). Tecnología Blockchain: Desafíos presentes y futuros en su aplicación. *Revista Conocimiento Online*, (2), 258-273. <https://doi.org/10.25112/rco.v2.2859>
- Banafá, A. (2022, December 22). Blockchain 4.0. <https://www.bbvaopenmind.com/tecnologia/mundo-digital/blockchain-4-0/>
- Benmoussa, A., Kerrache, C. A., Calafate, C. T., & Lagraa, N. (2023). NDN-BDA: A Blockchain-Based decentralized data authentication mechanism for vehicular named data networking. *Future Internet*, 15(5), 167. <https://doi.org/10.3390/fi15050167>
- Bitcoin.es. (2020, November 17). Vamos por la 5ta generación de la Blockchain ¿Cuáles son? <https://bitcoin.es/actualidad/vamos-por-la-5ta-generacion-de-la-blockchain-cuales-son/>
- Brooks, D. (2020, February 9). Criptomonedas: Qué es el "problema de los generales bizantinos" y por qué explica el origen del bitcoin. <https://www.bbc.com/mundo/noticias-51380491>
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and informatics*, (36), 55-81. <https://doi.org/10.1016/j.tele.2018.11.006>
- Castro, M., & Liskov, B. (2001). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, (20)4, 398-461. <https://doi.org/10.1145/571637.571640>
- Choi, T.-M., & Siqin, T. (2022). Blockchain in logistics and production from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizational framework. *Transportation Research Part E: Logistics and Transportation Review*, (160), 102653. <https://doi.org/10.1016/j.tre.2022.102653>

- Conoscenti, M., Vetrò, A., & De Martin, J. C. (2017). Peer to peer for privacy and decentralization in the internet of things. In *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), Buenos Aires, Argentina* (pp. 288-290). <https://doi.org/10.1109/ICSE-C.2017.60>
- Criptodemy. (2023, January 20). Guía sobre algoritmos de consenso Blockchain. Criptodemy ®. <https://criptodemy.com/guia-algoritmos-consenso-blockchain/>
- Guo, J., Wang, M., Chen, B., Yu, S., Zhang, H., & Zhang, Y. (2019). Enabling Blockchain applications over named data networking. In *2019 IEEE International Conference on Communications (ICC), Shanghai, China* (pp. 1-6). IEEE. <https://doi.org/10.1109/ICC.2019.8761919>
- Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. In A. J. Menezes & S. A. Vanstone (Eds.), *Advances in Cryptology-CRYPTO' 90* (pp. 437-455). Springer. https://doi.org/10.1007/3-540-38424-3_32
- Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, (2), 130-139. <https://doi.org/10.1016/j.ijin.2021.09.005>
- Hasan, M. K., Akhtaruzzaman, Md., Kabir, S. R., Gadekallu, T. R., Islam, S., Magalingam, P., Hassan, R., Alazab, M., & Alazab, M. A. (2022). Evolution of industry and Blockchain era: Monitoring price hike and corruption using BloT for smart government and industry 4.0. *IEEE Transactions on Industrial Informatics*, 18(12), 9153-9161. <https://doi.org/10.1109/tii.2022.3164066>
- Hong, L., Zhang, K., Gong, J., & Qian, H. (2022). A practical and efficient blockchain-assisted attribute-based encryption scheme for access control and data sharing. *Security and Communication Networks*, (2022), 4978802. <https://doi.org/10.1155/2022/4978802>
- Hurtado, J. S. (2021, July 1). Qué son las DLT y en qué se diferencian de Blockchain. <https://www.iebschool.com/blog/que-son-las-dlt-y-en-que-se-diferencian-de-blockchain-digital-business/>
- Kharjana, M., Pohrmen, F. H., Sahana, S. C., & Saha, G. K. (2023). Blockchain-based key management system in named data networking: A survey. *Journal of Network and Computer Applications*, (220), 103732. <https://doi.org/10.1016/j.jnca.2023.103732>
- Konkin, A., & Zapechnikov, S. (2023). Zero knowledge proof and ZK-SNARK for private blockchains. *Journal of Computer Virology and Hacking Techniques*, (19), 443-449. <https://doi.org/10.1007/s11416-023-00466-1>
- Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. *Sensors*, 22(14), 5274. <https://doi.org/10.3390/s22145274>
- Leka, E., Selimi, B., & Lamani, L. (2019). Systematic literature review of blockchain applications: Smart contracts. In *2019 International Conference on Information Technologies (InfoTech)* (pp. 1-3). IEEE. <https://doi.org/10.1109/InfoTech.2019.8860872>
- Lorenzo, C. (2020). Blockchain for copyright and intellectual property protection. In *Handbook of research on emerging business models and managerial strategies in the nonprofit sector* (pp. 180-198). IGI Global.

- Martínez-Ríos, F. O., Marmolejo-Saucedo, J. A., & Abascal-Olascoaga, G. (2020). A new protocol based on blockchain technology for transparent operation of corporate social responsibility. In S. García-Álvarez & C. Atristain-Suárez (Eds.), *Strategy, power, and CSR: Practices and challenges in organizational management* (pp. 205–233). Emerald Publishing Limited. <https://doi.org/10.1108/978-1-83867-973-620201012>
- Ministerio de Tecnologías de la Información y Comunicaciones [Mintic]. (2022). *Guía de referencia de Blockchain para la adopción e implementación de proyectos en el Estado colombiano*. Mintic. https://gobiernodigital.mintic.gov.co/692/articles-161810_Ley_2052_2020.pdf
- Mohaisen, A., & Kim, J. (2013, December 22). The Sybil attacks and defenses: A survey. <https://arxiv.org/abs/1312.6349>
- Moran, T., & Orlov, I. (2019). Simple proofs of space-time and rational proofs of storage. In A. Boldyreva & D. Micciancio (Eds.), *Advances in Cryptology—CRYPTO 2019* (pp. 381–409). Springer International Publishing. <https://eprint.iacr.org/2016/035.pdf>
- Mougayar, W. (2016). *The business Blockchain: Promise, practice, and application of the next internet technology*. Wiley.
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
- Ortega Llorente, P. O. (2023). Estudio comparativo de algoritmos de consenso para una Blockchain orientado al consumo de energía [Bachelor's thesis, Universidad Politécnica de Madrid]. Repositorio UPM. https://oa.upm.es/75158/1/TFG_PABLO_ORTEGA_LLORENTE.pdf
- Pérez Solà, C., & Joancomartí, J. (2014). Bitcoins y el problema de los generales bizantinos. In R. Álvarez Sánchez, J.-J. Climent Coloma, F. Ferrández Agulló, F. Martínez Pérez, L. Tortosa Grau, J. F. Vicent Francés, A. Zamora Gómez (Coords.), *Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información RECSI XIII: Alicante, 2-5 de septiembre de 2014* (pp. 241–246). <https://rua.ua.es/dspace/handle/10045/40461>
- Popchev, I., Radeva, I., & Velichkova, V. (2021). Blockchains in enterprise global risk management. In *2021 International Conference Automatics and Informatics (ICAI)* (pp. 282–287). IEEE. <https://doi.org/10.1109/ICAI52893.2021.9639500>
- Raikwar, M., & Gligoroski, D. (2021). R3V: Robust round robin VDF-based consensus. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 81–88). IEEE. <https://doi.org/10.1109/BRAINS52497.2021.9569781>
- Relictum Pro. (n.d.). Is blockchain 5.0 of the latest generation. <https://relictum.pro/>
- Romero Ugarte, J. L. (2018). Distributed ledger technology (DLT): Introduction. *Economic Bulletin*, (4) 2–11. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269731

- Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences*, 9(9), 1788. <https://doi.org/10.3390/app9091788>
- Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electron Markets*, (32), 1779-179. <https://doi.org/10.1007/s12525-022-00536-0>
- Soto, M. G. (2018, August 6). El problema de los generales bizantinos (PGB). <https://marvin-soto.medium.com/el-problema-de-los-generales-bizantinos-pgb-e0cb8c4279c2>
- Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE Network*, 35(4), 198-205. <https://doi.org/10.1109/MNET.011.2000473>
- Swan, M. (2015). *Blockchain: Blueprint for a New Economy* (1st ed.). O'Reilly Media, Inc.
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World*. Penguin.
- Vamsi_Cz5cgo. (2016, January 28). The Architecture of Blockchain (4/5). <https://www.vamsitalkstech.com/blockchain/the-architecture-of-blockchain-45/>
- Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, 5, 27. <https://doi.org/10.1186/s40854-019-0147-z>
- Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain Technology? A systematic review. *PLoS ONE*, 11(10), e0163477. <https://doi.org/10.1371/journal.pone.0163477>
- Zheng, J., Huang, H., Zheng, Z., & Guo, S. (2023). Adaptive double-spending attacks on PoW-based Blockchains. In *IEEE Transactions on Dependable and Secure Computing* (pp. 1-13). IEEE. <https://doi.org/10.1109/TDSC.2023.3268668>

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 operations¹ 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*

Process	Function	Objectives	Process management
Logistics planning	Lead logistics through the creation of strategies and their alignment in the organization	To control and measure logistics management, production, supply, maintenance, technical services, and transportation	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
Acquisition of goods and services	Identify needs, select purchase mode, and administer the useful life of the good or service for the sustainability of the Army	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	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

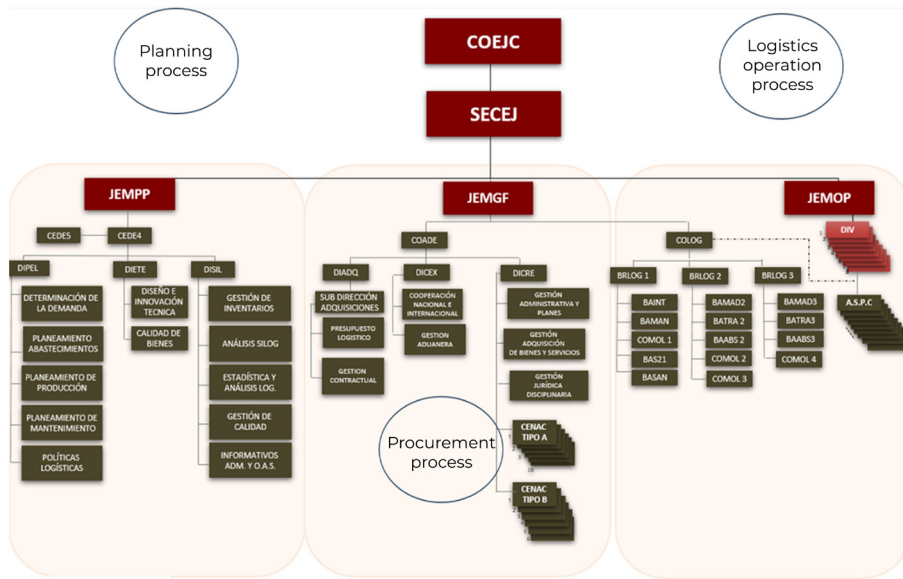
Logistics operation	Part of the supply chain that consists of calculating, preparing, arranging, organizing, delivering, and monitoring materials, goods, and services from the point of origin to the point of consumption, and meeting the needs for the functioning of an Army and its operations	To guarantee 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.
<ul style="list-style-type: none"> • Purchasing • Inventory management • Production • Sales • Acquisition plan • Quality 	<ul style="list-style-type: none"> • Aeronautical • Naval • Land • Biomedical • Weapons • Communications • Human resources 	<ul style="list-style-type: none"> • Fixed assets • Accounting • Budget • Costs • Treasury
<p>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.</p> <p>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.</p> <p>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.</p>		

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 logistics² and cyberspace³ 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 Technology⁴

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 Cybersecurity⁵

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 Theory⁶

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 Resilience⁷

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*

	STRENGTHS	WEAKNESSES
SWOT ANALYSIS	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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
	SO STRATEGIES	WO STRATEGIES
OPPORTUNITIES	<ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 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
<ul style="list-style-type: none"> • 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 	<ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 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.>
- Ganuzá, 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 ciencia política: La metodología 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. *Enseñanza 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-teorla-y-mAs-acciOn>

Chapter 4

Cutting-Edge Sciences and Disruptive Technologies in Cyberspace as a Framework and Condition for Colombia's Cyber Defense*

DOI: <https://doi.org/10.25062/9786287818064.04>

Carlos Eduardo Maldonado

Universidad el Bosque

Abstract: This chapter examines the significance of complexity sciences, exploring its various lines, themes, and challenges within the context of our increasingly digital world and society. It highlights the implications for national security and defense, arguing that complexity sciences are essential life sciences that address issues often overlooked by traditional science. Additionally, the chapter points out a critical tension between science and technology: While science typically embodies democratic principles, the history of technology has frequently focused on *prima facie* military applications. Ultimately, it concludes that complexity sciences offer a means to navigate and resolve this tension.

Keywords: complexity sciences; computing; digitization; life

* 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

Carlos Eduardo Maldonado

Visiting Postdoctoral Scholar, University of Pittsburgh, United States. Visiting Postdoctoral Research Professor, Catholic University of America, United States. Academic Visitor, School of Philosophy, University of Cambridge, England. Doctor of Philosophy, K. U. Leuven, Belgium. Professor, Universidad El Bosque, Colombia. Professor, Universidad del Rosario.

<https://orcid.org/0000-0002-9262-8879> - Contacto: maldonadocarlos@unbosque.edu.co

APA Citation: Maldonado, C. E. (2025). Cutting-Edge Sciences and Disruptive Technologies in Cyberspace as a Framework and Condition for Colombia's Cyber Defense. In M. E. Realpe Díaz & A. M. González González (Eds.), *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* (pp. 99-128). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818064.04>

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

The entire history of technology is, *prima facie*, military technology specifically for defense, protection, control, attack, and security. The history of technology effectively encapsulates the history of warlike military technology; they amount to the same thing. From the invention of fire to the wheel, the knitting or spinning needle, and the axe, right up to recent days, with one notable exception: the birth of the internet. While various attempts at the origins of the internet had a military intention—such as the entire history of Arpa in 1958, followed by the history of Arpanet in 1969—the internet was born as a distinctly civil matter, aimed at benefiting humanity, thanks to CERN—the European Organization for Nuclear Research—in 1989. This fact marks a unique turning point in the entire history of technology.

Various States, forces, and corporations have tried to control the internet, with different motivations and justifications. It is simply impossible. However, the majority of society still ignores these processes, attempts, and policies, as well as the intelligent use of the internet. Perhaps, the best expression of attempted control over the internet is the Eschelon network (Maldonado, 2019a). Control or the impossibility to control the internet is part, without the slightest doubt, of one of the most critical aspects of complexity, the world, and knowledge. The complexity of the world and knowledge? The question immediately refers to complexity sciences.

This chapter presents and discusses the most significant articulations of complexity sciences, generically also called *cutting-edge sciences*, in stark contrast to normal, hegemonic, or classical science, three different ways to point in the same direction. The “dominant paradigm,” Thomas Kuhn would say, in an expression—paradigm—with which he later disagreed, against which Kuhn would have highlighted either the idea of “new paradigm(s)” or, much better, the scientific revolution.

Moreover, since its birth in ancient Greece—specifically during the transition from archaic Greece to classical Greece—science has always implied democracy, an implication that is neither easy nor direct, as we will see later. Indeed, science emerged in classical Greece after the Thirty Tyrants, thanks to the governments of Solon and Pericles. The humanists first appeared, particularly the sophists, with whom Plato and Aristotle engaged in debate. Subsequently, the finest aspects of philosophy, astronomy, geometry, logic, arithmetic, and medicine were developed, along with the best of the arts. The history of the relationship between science and democracy has been extensively documented throughout history and geography.

Thus, we are witnessing an essential tension. It is the tension between science and technology, one markedly democratic in the philosophical sense of the word. This sense is condensed in the expression *logos didomai*, which in Greek means both to ask for or demand reasons and to give or provide reasons, which was initially done in the public square, in the agora. It then gets technical at the Lyceum and Academia. On the contrary, technology, in general, has a distinctively belligerent, defensive, and warlike spirit in the sociological meaning of the word.

The entire history has involved tension and complementarity, depending on the case and the moment between science and technology. Significantly, when T. Kuhn wrote his famous book on scientific revolutions in 1962, the ratio of scientific revolutions to technical or technological revolutions was one to four; that is, for each theoretical or conceptual revolution, there were four technical or technological revolutions. It is sufficient to remember, let us mention in passing, that the revolution of Watson and Crick and the discovery of the structure of DNA, vital as it is or as it was, was not a theoretical revolution but a technical or technological one. Well, by 2012, the ratio of scientific revolutions to technological revolutions had increased to one to seventeen.

We are witnessing an enormous advance in knowledge, but the vast majority of these advances are technical and minimalist. We need a magnificent theoretical or conceptual revolution, but this is not the place to delve into it.

Plain and simple, we are engaging in many activities without necessarily understanding what we are doing, their consequences, or the broader frameworks and contexts of our actions (the big picture). Alternatively, it appears that knowledge management in general is less concerned with the theoretical dimension of knowledge—that is, basic research—and favors experimental and applied research much more effectively.

Whatever the case, today, two things no longer exist: science, on the one hand, and technology, on the other. Not in vain, G. Hottois consequently coined the concept of *technoscience*. Technologies acquire the much more appropriate mantle of engineering. And engineering is an applied science.

This work revolves around complexity sciences, their importance, and their meaning, in this case, security and defense studies. From the emergence of liberalism, on the one hand, and the subsequent constitution of the nation-state, security and defense issues were generally abrogated to the State and the relevant agencies and forces.

Well then, since their origins in Locke, Hobbes, and notably, Rousseau, security and defense issues refer to the protection and care of life. Not the State or a type of government. (We should revisit the classics of liberal thought.) Thus, the thesis of this chapter is that cutting-edge sciences and technologies that are highly necessary and relevant for the care and affirmation of life exist and are being developed. We must be able to know and take ownership of them, all of us. In Colombia, these sciences and technologies are still widely unknown to all the government and state sectors. A careful look would be enough, from the Conpes documents to the development programs (PNDs, by its Spanish acronym), from the different jurisprudence of the High Courts to the most sensitive documents of the Military and Police Forces, or from the declarations and records of the episcopate to the most important centers of the private sector, such as Andi, and many more; in short, from the laws enacted in the Congress of the Republic to the documents of the different science and technology missions that have taken place, for example. To date, complexity sciences remain a dish typical of the academic and scientific communities. The closest some have come is to systems thinking. And that still is very far from complexity. This is the novelty of this text.

Scientific and Technological (or Industrial) Revolutions

The expression *cutting-edge sciences* is a generic way of indicating a range, a mosaic of sciences and disciplines, of techniques and technologies, increasingly intertwined, that have been emerging strongly. Today, there is a very evident advance in knowledge. New sciences, disciplines, technologies, and understandings are increasingly emerging. The reason is straightforward: There has never been in

the history of humanity the number of mathematicians, biologists, engineers, and others that there are today. And there have never been so many people with master's degrees and doctorates. Something similar could be said in many areas. We live, literally, in an age of light.

Understanding science and technology involves openly presenting the three scientific revolutions that have occurred to date (Maldonado, 2020a). The first is the revolution of classical or modern science, whose two apices are the Copernican revolution and the development of classical mechanics, a work that goes from Galileo to Newton; and with Newton, more recently, the development of statistical mechanics in the 19th century with the works of Maxwell and Gibbs. The First Scientific Revolution took four centuries and produced significant constructions, classical mechanics, thermodynamics, microbiology, and all the social and human sciences based on the program formulated by A. Comte, the father of positivism, and with many difficulties, biology. Roughly speaking, it covers the works of Bacon, Descartes, and Galileo until 1905, exactly. At the end of classical science, ecology began to be born.

At the level of technology, it was the steam engine, invented by Watt in 1769, and the subsequent mechanization of work and society that gave rise to the First Industrial Revolution. The mechanization of society increasingly extended to practically all levels of society.

The Second Scientific Revolution extends from 1900 to the present, encompassing quantum theory. This period includes quantum physics, quantum chemistry, all technologies based on quantum principles or behavior, quantum biology, and, more recently, quantum social sciences (Maldonado, 2019b). Quantum theory can be divided into two phases. The first, the classical phase, spans from 1900 to 1934, highlighted by the famous EPR paper authored by Einstein, Podolsky, and Rosen. The second phase includes the works of Bohm and Feynman up to the present day, leading to advancements in quantum computing, quantum information processing, teleportation, the study of tunneling phenomena, and cryptography. The division between these periods of quantum theory is marked by the emergence of nuclear physics after World War II, particularly with the Manhattan Project and the subsequent developments during the Cold War, culminating in the creation of a hydrogen bomb by the USSR in 1952.

The Second Scientific Revolution took decades to carry out. On the technological scale, the most essential phenomenon was the birth of the computer and computing, not without precedent, thanks to A. Turing. Without a doubt, computers are the most

critical tools and technologies ever developed by humans, even above the mastery of fire and the invention of writing, the wheel, or the knitting or spinning needle.

Finally, the Third Scientific Revolution began in 1948 with the famous article by Shannon and Weaver. It is about the information revolution that extends to this day, giving rise to social networks, all born around 2012. This revolution takes years to take place.

Technologically, the Second, Third, and Fourth Industrial Revolutions occur almost simultaneously.

The Second Industrial Revolution consisted of mass production and began in the 1910s within the framework of World War I. It was formulated in 2011 and centered on the importance of the internet, which gave birth to artificial intelligence. The Third Industrial Revolution was identified in 2016 and consists of the synthesis of the physical, biological, and digital dimensions of the world and society.

There is a distance between the First and Second Industrial Revolutions regarding the Third and Fourth Industrial Revolutions, and, at the same time, there is a tendency toward approximation between them.

Well, there is, at the same time, an increasing distance between the Second and Third Scientific Revolutions and a rapprochement between the Third and Second Scientific Revolutions.

This is the broad panorama of science and technology. However, some significant peculiarities also take place. The most important may be the following.

Around the 1960s, new sciences were born—note the plural—based on border problems. Chronologically, these sciences as a synthesis are the following:

Cognitive Sciences

They were initially born in the MIT MediaLab around the 1960s. They are defined by a problem, namely, what knowledge is, for which they introduce a neologism, cognition, to differentiate it from knowledge. While this is clearly anthropological, cognition serves to designate a problem consisting of the fact that bacteria, plants, and animals know, just like human beings, but computers are also susceptible to knowledge.

Earth Sciences

In the 1970s, an idea formulated in the 1930s by Wegener was confirmed: plate tectonics and continental drift. The Earth is a dynamic system. At the same time, the exploration of outer space, a research program inaugurated by the former Soviet Union, shows that there may be other planets like Earth. Exobiology,

astrochemistry, and astrophysics were born. In 1964, cosmology was born as a science, known as the Big Bang inflationary theory.

Space Sciences

Closely related to the previous ones, space sciences consist of dual research into outer space in the search for exoplanets and exploration of the ecosystem in which the solar system and, in turn, the Milky Way are located. From a terrestrial perspective, they observe whether biogeochemical cycles eventually exist. Black holes and the search for understanding the origin of the universe constitute some of the most critical issues.

Health Sciences

After the birth of scientific medicine in 19th-century physiology, a magnificent emergence of sciences and disciplines linked to medicine and the study of disease occurred. On the one hand, all the medical-clinical and medical-surgical specializations, and on the other, the birth of related fields and the strengthening of the pharmaceutical industry constitute a fantastic dimension with enormous achievements in numerous fields to date.

Materials Sciences

From the 1980s to date, progress in physics and materials engineering has not ceased, impacting all areas of societal life. Currently, graphene is of singular importance, permeating the best of technoscience. Nanotechnology plays a unique role in this spectrum.

Life Sciences

Closely linked to health sciences, life sciences consist of the hybridization among geology, microbiology, paleontology, botany, and physical geography. It is practically impossible to turn your head and not find life, from extremophiles to viruses and bacteria on a human scale. Importantly, beyond the human scale, it has recently been about artificial intelligence and life.

Complexity Sciences

In 1984, complexity sciences were born, to which we will return in the following section, to study non-linear dynamics that are radically different from all classical or modern science. After their birth, spaces expressly dedicated to studying systems of increasing complexity were created in the most important research centers and institutes, universities, national government bodies, and occasionally, the private sector.

It is essential to highlight numerous links among the sciences indicated, possibly from boundary problems.

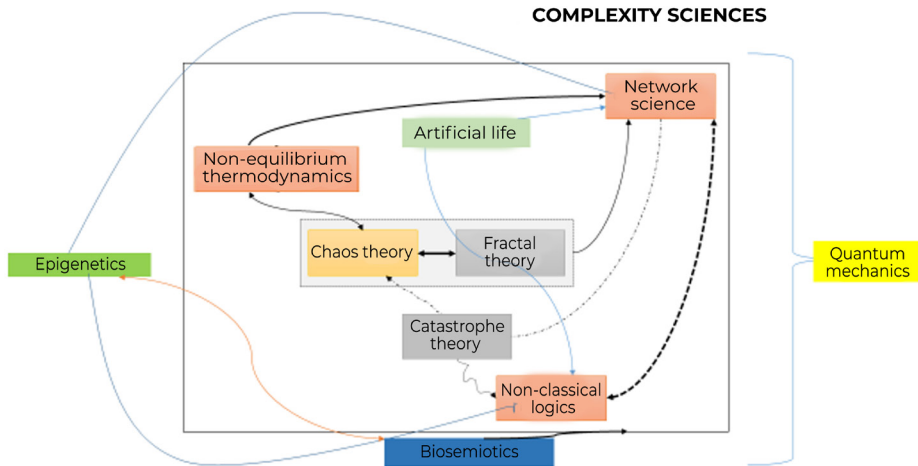
Furthermore, on another level, between the end of the 20th century and the beginning of the 21st century, convergent technologies appeared. These are known by the acronym NBIC+S, which stands for nanotechnology, biotechnology, information technologies, cognitive science, and the social dimension of technology. (Talking about ICT today is an archaism, to say the least.)

In summary, a scientific revolution is not just a shift in understanding, but a transformative change in the worldview and our comprehension of the world, nature, the universe, and the human being himself. Similarly, an industrial revolution is not just a reorganization of work, but a profound transformation that reshapes society and its structures.

Complexity Sciences. Characterization

Complexity sciences were born, conceptually and semantically, in 1984. However, its origins go back, *avant la lettre*, to the discovery of calculus by Leibniz and Newton, to the contributions of Gödel and Turing, and the always inevitable impact of the different works, as they are from each other, of Hilbert and Poincaré. This work does not want to elaborate on the history of the direct and indirect antecedents of complexity sciences. Instead, it is about its characterization and its specificity. That said, it must be clear that all cutting-edge research in the world (spearhead science) passes fundamentally through complexity sciences. Understanding them is a *sine qua non* for their study and implementation at any level or context. Figure 1 presents an overview of complexity sciences.

Figure 1. Overview of Complexity Sciences



Source: Own elaboration.

The first of the complexity sciences, chaos theory, is characterized by its showing that the complexity of a phenomenon, system, or behavior consists of its unpredictability. Born in the context of meteorology, chaos not only makes it evident that things generally are, sooner rather than later, unpredictable and that unpredictability cannot in any way be ruled out, as it makes chaos an explicit theme of study and research.

A chaotic system is a highly ordered system, but one that is unpredictable. Are there phenomena and behaviors that are predictable? That is, moderately or approximately predictable? Of course. Complexity does not work there. Other tools for this type of predictable phenomenon have absolutely no complexity, such as planning, foresight, and probability studies and theory. Unpredictability means that things can be predictable only in the short term, and the shorter the term, the better. However, phenomena are increasingly unpredictable in the medium and long term. From meteorology, the study of chaos extends to natural, social, or human phenomena and behaviors.

That said, not all things are complex. What is more, the vast majority of things are not. Complexity sciences work only on those phenomena that can be identified as complex, that is, of increasing complexity. So, for the question: What is complexity, and why does it arise? There is an immediate (first) answer: due to the unpredictable nature of things. Thanks to chaos theory, we are doing science of unpredictability for the first time in the history of humanity.

In the 1970s, fractal geometry emerged contemporaneously with chaos theory. It is the explicit recognition that nature has a fractal dimension, in contrast to the classical way of understanding natural phenomena based on Euclidean geometry. More precisely, fractal geometry consists, put succinctly, of a double characteristic. On the one hand, the fractal dimension means that the structure of a part corresponds to the structure of the whole; technically, this is called *self-similarity* and is the subject of mathematical measurements, essentially based on iterations.

Conversely, fractal geometry also implies that nature is irregular. These irregularities give food for thought within the framework of this geometry and demand the ability to see irregularities, patterns, and pattern breakouts. Fractal geometry has been used to study human, natural, and artificial systems, notably technological systems.

Having said that, it is necessary to note that there are innumerable geometries and that each geometry describes its own separate world. In a fortunate but fortuitous circumstance, let us say that in 1977, another complexity science was born: catastrophe theory. Catastrophe is the term used in a theory of mathematical origin to designate sudden, unforeseen, irreversible changes. As can be seen immediately, it is not in the interest of complexity sciences to study trends, vectors, or matrices. Quite the contrary, it is about studying dynamics, changes, spaces, and processes that take place suddenly, are or can be irreversible, and are, therefore, unforeseen. It is not difficult to see the connections among several complex sciences.

Although it is not the direct subject matter of this work, it must be said immediately that the mathematics of complexity is not the mathematics of continuous systems. Quite the contrary, it is the mathematics of discrete systems. This means that, on the one hand, average statistics—normal, Gaussian, Poisson, Bernoulli, gamma, and other distributions—are not in the interest of complexity in any way. Likewise, fields such as calculus, difference equations, the notion of limits, the study of functions, and others are not considered by complexity. A deepening and appropriation of the mathematics of discrete systems must be possible.

In 1977, I. Prigogine received the Nobel Prize in chemistry for his contributions to non-equilibrium thermodynamics and for having introduced into science what science did not have: time (Prigogine, 2003). Complex systems, as non-equilibrium thermodynamics reveals, are open systems—closed or isolated systems do not exist or are not possible. The most important thing that happens to them is the arrow of time, namely, the arrow of a growing time, ultimately generating life.

Equilibrium, in any sense and context, is always provisional. More appropriately, we should speak of the absence of equilibrium or, what is equivalent, of dynamic equilibrium. The technical term used to designate this class of phenomena and systems is dissipative structures.

While time was a factor that was always discarded in the study of world affairs, Prigogine's studies show that complexity exists precisely because of time. This cannot be considered a framework of probabilities or a taken-for-granted issue. Instead, time is the generator of non-equilibrium—in a word, non-linear—dynamics.

Furthermore, the thermodynamics of phenomena far from equilibrium shows that dissipative structures are self-organizing. That is, the essential things in the world and nature are not subject to a control system, in any sense of the word, but spontaneous and, in themselves, robust. Self-organization is a fundamental approach that is part of complexity sciences (Camazine et al., 2003).

Another field of complexity science is artificial life. Established in 1989 at the initiative of C. Langton, it is a purely philosophical program that utilizes computing. The purpose of artificial life is to comprehend what life is, how it arises, its dynamics and logic, and how, in its origins, artificial intelligence similarly explored the mind or intelligence through the development of the Turing machine. Thus, without the slightest doubt, artificial intelligence and artificial life represent two sides of the same coin.

This observation allows us to highlight that complexity sciences are the result of computing and, in turn, actively constitute the development of computing (Pagels, 1991).

In this regard, working with complexity is distinctively working with computing, plain and simple, as a tool, namely, the best tool developed to work with possibilities.

Complexity does not concern itself with what is real, what is at hand, and what exists in any sense of the word. For that, you do not need complexity. Regular science suffices. On the contrary, the most important of all the methodological and heuristic features of complexity sciences is that they study the phase spaces of actual phenomena. This means that it involves learning about the spaces of possibilities for the evolution of any phenomenon. We will never understand anything if we ignore phase spaces. Technically speaking, these phase spaces are known as the Hilbert space, named after D. Hilbert. Another interpretation of phase spaces, which allows for working with first- and second-order phase transitions, is as the adjacent possible.

Therefore, in any sense of the term, the real appears only as a subset of a more extensive set that comprehends it and makes it possible, namely, the world of possibilities—of possibilities and not of probabilities. After all, contemplating what is possible even entails considering impossibilities. Complexity sciences are a science, even of the impossible. We are engaging in the science of the impossible today (Maldonado, 2021).

From 2001 to 2003, a new field of complexity science emerged: network science. In this way, the complexity of a phenomenon depends on the networks it is part of or that it creates. Complex networks fall into three categories: small-world, random, and scale-free. We live in a highly interconnected world in numerous ways, and it is these networks that enable us to understand complexity; for example, the unpredictability of sudden, unforeseen changes or the absence of equilibrium.

Perhaps the greatest discovery of network science is the phenomenon of synchrony or synchronization, which occurs at all scales of nature, even in inanimate physical systems. This synchronization is technically known as the *Kuramoto effect*. Synchrony is a spontaneous phenomenon that does not require centrality or hierarchies to be understood.

A fortiori, synchronicity phenomena exist in natural systems as well as in human systems. Complexity permeates nature and, therefore, non-linearity.

This is the greatest difficulty that complexity sciences, along with their technologies and tools, pose for a classically formed mental structure. There are spontaneous dynamics (order-for-free, in technical language). Some bottom-up self-organization phenomena do not require a top-down approach. This topic is directly and necessarily related to topology, which, if the expression fits, serves as the mathematical basis of complexity.

As can be easily seen, it is a series of structures, dynamics, and processes that have nothing to do with classical culture: emergencies, non-linearity, self-organization, synchronization, spontaneous order, absence of hierarchy, and centrality. These traits and mental frameworks enable us to understand why most companies, states, and government agencies worldwide recognize complexity and have learned about it in some way, yet struggle to adopt, implement, and deploy it fully. Clearly, this represents a scientific revolution.

A common feature of all complexity sciences appears immediately after the panorama presented above, before a sensitive gaze. Complexity consists of perceiving phenomena, dynamics, processes, or structures as living systems or systems that exhibit life. In contrast to all classical science, it is decisively

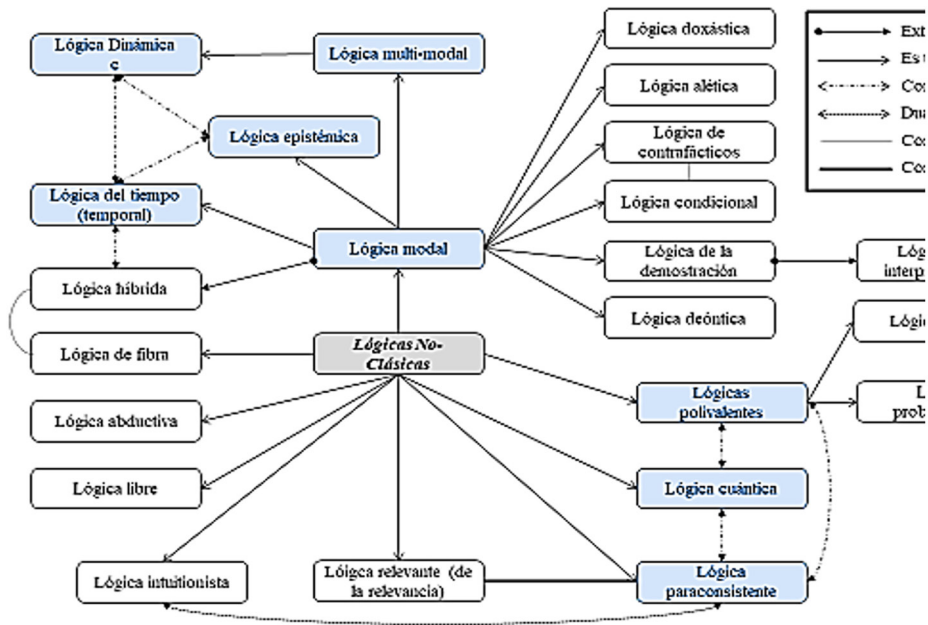
mechanistic and deterministic—a radical transformation of any perspective in any plane or context you choose.

Additionally, following Figure 2, another complexity science is non-classical logics (NCLs). It must be said that this idea is specifically Latin American in general and constitutes one of the contributions of Latin America to the history of science, for example, analogous to the concept of autopoiesis of Maturana and Varela or the paraconsistent logics of N. da Costa or the economies of scale, initially introduced by M. Max Neef—barefoot economies, Max Neef called them—for example. No one else, neither on the side of the logicians nor on the side of the complexologists, ever saw or established this relationship.

NCLs constitute a broad continuum of alternative logic, most of which are complementary to classical formal logic, also called *standard logic*. This logic can be designated in four ways: mathematical logic, propositional logic, symbolic logic, or predicate logic. It is, in any case, first-order logic.

NCLs immediately recognize that a logical pluralism exists, a pluralism of systems of truth. In other words, there is no single truth. This is undoubtedly a cause for scandal for the classical vision. Figure 2 illustrates the NCL landscape.

Figure 2. Overview of Non-Classical Logics (NCLs)



Note. Figure 2, however, does not intend to be exhaustive.
 Source: Own elaboration based on Maldonado (2020b).

The fundamental idea is that there is logical pluralism. Therefore, several worlds are possible, logically speaking. It is important to note that the semantics of NCLs reflect the semantics of possible worlds. Thus, the idea that thinking and working with complexity involves engaging with possibilities and even impossibilities is understood and reinforced.

Such is, so to speak, the classic panorama of complexity sciences in brief. There is a proper way to understand them, put negatively. Complexity sciences can be ideally understood as rejecting any form of dualism, determinism, mechanism, or reductionism.

Well, in precisely this same atmosphere and spirit, two sciences—epigenetics and biosemiotics—can ideally be included among complexity sciences.

Epigenetics, not without precedent, emerged in 2005 and merits recognition for overcoming the culture-nature duality. We not only inherit and transmit genes; we also inherit and communicate experiences. By 2005, it was established that this phenomenon occurs across up to three generations. By 2021, it was established that this process spans up to eight generations. Epigenetics has been confirmed in plants, animals, and humans.

It is easily understood that the split between natural sciences and human sciences, or between exact sciences and arts, or even between nature and culture, is now perfectly unsustainable. Any action or decision on one plane immediately affects the other plane.

For its part, biosemiotics is articulated in three main domains: anthroposemiotics, zoosemiotics, and phytosemiotics. In all cases, the focus is the production of signs, signals, codes, patterns, and messages at the levels of living systems. Living systems read signs and signals, interpret them, and subsequently create new signals and messages, thereby forming a vast informational field that traverses, constitutes, and elucidates the dynamics of living systems in general: plants, animals, and human beings, overall.

Whatever the case, looking to the left of Figure 1 is essential. It pertains to quantum mechanics. Quantum mechanics is, without a doubt, the archimedical fulcrum of the world's entire scientific and technological edifice today. It is the most robust, the most conforming, the most verified, and the most falsified of all scientific theories. It has been confirmed and falsified to the eleventh decimal: 0.0000000001. No theory has such solidity.

Quantum mechanics is (straightforwardly) a very technical and challenging mathematical device dedicated to studying quantum phenomena and behavior. These phenomena are characterized, among other features, by non-locality,

superposition, indeterminacy, complementarity, entanglement, teleportation, tunneling, and Pauli exclusion. Evidently, this is a highly counterintuitive theory that is based on something other than the weight of natural perception or the senses.

Quantum mechanics is the most advanced theory developed to explain phenomena such as the universe, the world, nature, human beings, and life in any meaning or sense of the word. Simply put, it is impossible today to provide an explanation, gain an understanding, much less make a decision, without at least a basic but solid knowledge of quantum mechanics.

Let us put it bluntly: cutting-edge sciences, in general, and complexity sciences, in particular, are impossible outside of quantum mechanics. This is precisely articulated in five domains: physics, chemistry, technologies, biology, and quantum social sciences.

It would be desirable to present the disciplines and approaches of complexity sciences. For example, swarm intelligence indicates that, in nature and natural systems, there are instances when groups choose to act as individuals because, in this manner, they achieve better outcomes than if they worked collectively. Schools, birds, social insects, subatomic particles, and gazelles are notable examples. Human beings have yet to fully learn these behaviors, especially those influenced by Western ways of thinking and living.

Likewise, reference should be made to the concept and emergency processes. Thinking in complexity is the complete opposite of thinking in terms of causality and even multicausality; its variants include “multivariate or multidimensional analysis” and others. Emergent properties or behaviors mean no proportionality between the input and the output. The output is much more than, and very different from, the input.

A final observation is in order. *Systemic* is perfectly different from *complex*, a rampant confusion that prevails out there, even in the scientific and academic world. This is not the place to underline demarcation criteria (Maldonado, 2023a).

Whatever the case, a prominent family trait permeates and defines complexity sciences. It involves thinking about phenomena as living systems or, equivalently, as systems that exhibit life. This idea has very serious epistemic and moral consequences.

Mathematical Tools of Complexity

Complexity sciences are essentially two things. On one hand, they represent a robust epistemological apparatus composed of various sciences, disciplines, approaches, and understandings. A brief overview has just been outlined. At the same time, they consist of sophisticated techniques and tools, which I deal with below.

As an introduction to this section, it must be noted that there are three types of science today that correspond to three distinct methods or methodologies. These are science by induction, science by deduction—which correspond to the scientific models of the First Scientific Revolution—and science by modeling and simulation. Accordingly, one can speak generically of three primary scientific methods: qualitative methods, quantitative methods—occasionally mixed or hybrid methods that combine the above—and modeling and simulation.

Significantly, work in science, much more than in fields, areas, behaviors, or dynamics, consists of the discussion and development of models. There are three lines of work in this regard: 1) how a model arises or is formulated, 2) how a model is supported or maintained, and 3) how a model is dismantled. Naturally, it can be an economic, political, educational, financial, or other model. Thus, a taxonomy of models includes the following configurations:

A Conceptual Model

By default, this is, in principle, always included. It is about the elaboration that results from the clarification of a state-of-the-art. The model can be, generically speaking, a theoretical or conceptual model. In research projects, it is precisely what is designated as the theoretical framework or conceptual framework. It is the minimum that reasonable research can or should have. It is the norm, in any case.

A Mathematical Model

There are, roughly speaking, two types of mathematics: the mathematics of continuous systems and the mathematics of discrete systems. Thus, the mathematical model includes two options. As mentioned, the mathematics of complexity is the mathematics of discrete systems. I will return to this idea below.

A Logical Model

There are two significant dimensions of logic: formal and non-classical (LNC). Consequently, a logical model allows for two possibilities. It all depends on the strength of innovation or the researcher's risk commitment. As mentioned, LNCs will enable a variety of options. In this regard, everything depends on the capabilities of each researcher.

An Informational Model

It refers to the use of existing programming languages. There are numerous programming languages for different uses.

A Computational Model

It refers not only to the use of a programming language but also to the development of code. That is, promising research must be able to write code to study and explain a phenomenon, problem, or system.

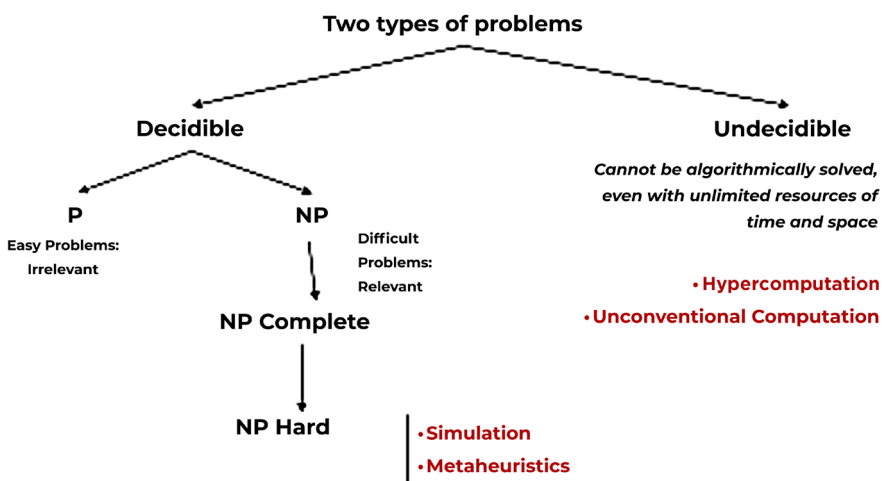
I would like to express this clearly. Research must include at least two of the previous models. By default, you already have one: the conceptual or theoretical model. Additionally, it should incorporate another one. Ultimately, it all depends on the strengths and learning capabilities of a researcher or research group.

That said, it is important to make a fine distinction, which is not difficult at all. Modeling is one thing, while simulation is quite another. Linear systems can be modeled, but only non-linear systems can be simulated. It is not impossible that there are links between modeling and simulation. In other words, the purpose of modeling is to apply or implement a model. For its part, the purpose of a simulation is to understand or explain a given system very well.

Without being exhaustive, I briefly present the main complexity tools below. It is worth noting that these are exclusive or distinctive tools of complexity sciences. Thus, it is essential to develop a mental structure based on the theoretical corpus (i.e., complexity sciences) and tools, rather than favoring one over the other.

The first fundamental tool is the theory of computational complexity. Figure 3 illustrates what it consists of.

Figure 3. Computational Complexity Theory



Source: Own elaboration based on Maldonado y Gómez (2011).

The basic idea is straightforward. All problems are resolved within a given time frame. The simplest way to designate the resolution times of a problem relates to computing (capacity) (concerning that problem). Thus, all issues in science or life can be categorized into two groups from this perspective: undecidable problems and decidable problems. The undecidability—or decidability—of a problem does not imply that it cannot be resolved or articulated. Instead, with undecidable issues, the focus is on the difficulty—better put, the impossibility—of solving them within a certain time and space, with any inputs, given an actual or potential algorithm. In other words, determining if and when a problem can be resolved is impossible since no algorithm exists or is likely to exist.

The distinction between decidable and undecidable problems is derived from D. Hilbert's tenth problem, known as the halting problem (*das Haltungsproblem*) (Gray, 2003).

Undecidable problems consequently call for non-conventional computing to understand and resolve them. Perhaps the most conspicuous case in this regard is biolohypercomputing, whose most complete expression is biological hypercomputing. Some examples of undecidable problems are inequality, poverty, knowledge, health, and life.

For their part, decidable problems are those that either have an algorithm or can develop one for their resolution, even if it does not exist yet. P refers to polynomial time, while NP refers to non-polynomial time. Technically, these are known as the P versus NP problems. These, in turn, are part of the Millennium Prize problems, which are the final problems in mathematics to be solved, according to the Clay Institute. The most fundamental expression of polynomial time is physical or chronological time, which can be managed through agendas, schedules, organizational charts, and other similar distributions. Explaining the derivations of NP problems in terms of hard and complete problems would be lengthy. However, the literature on the subject is extensive and, in many ways, not very technical.

Now, it is essential to point out that the theory of formal computational complexity is based on a more significant theory: the theory of complex problems (Maldonado, 2022). This assumption arises from the challenging issue of distinguishing which problems can appropriately be labeled as complex and why. Let us say it explicitly: not all problems are complex in the full sense of the word. Furthermore, most problems in science, as in life, are not rigorously complex.

Generally and classically, each science or discipline has a heuristic that consists of the ability to solve a problem. It is also frequently assimilated into the innovation

capacity of a science or discipline. However, between 1980 and 1990, a significant development occurred in the study of systems and behaviors characterized by complexity: the emergence of metaheuristics, a new and exciting addition to the toolkit of complexity.

Its most outstanding feature is the identification, with different criteria, some of which are technical, such as homeomorphisms, of groups of problems in search of solution spaces. The emphasis is on the plural.

Let us state it directly and precisely. In research, the delimitation of a problem is generally formulated—such as in terms of methodological delimitation and so forth—and this is considered normal science. Normal science does not aim to solve problems genuinely, but rather to shift or postpone them. The concept of scientific revolutions is well understood, whether from T. Kuhn's perspective or within the French tradition, as seen in the works of Koyré, Bachelard, and Canguilhem.

Metaheuristics, if you will, are much more effective, as they bring together groups of problems without limiting themselves to one problem at a time and seek solution spaces for problems that share similar criteria (Maldonado, 2013).

Metaheuristics, in turn, are articulated in a variety of approaches and strategies such as multilevel, hybrid, P, and NP—in direct connection with the P versus NP problems above, evolutionary, nature-inspired, local or global search, stochastic or sparse search, and several more metaheuristics. It is evidently a broad, suggestive, and distinctively complex terrain.

Furthermore, it has been said that the mathematics of complexity is the mathematics of discrete systems. Its main articulations include partially ordered sets (posets). Things in the world cannot always be resolved or ordered except provisionally and partially. This is what this chapter consists of. Additionally, the mathematics of complexity encompasses extreme sets, discrete and combinatorial geometry, discrete probability theory, all combinatorial problems, also known as combinatorial complexity, game theory—including evolutionary games—and rational decision theory, topology (already mentioned), some of the NCLs, and all the mathematics of computing systems, which includes graphs and hypergraphs.

It is apparent that this is a large and suggestive arena. Therefore, it is evident that these are disruptive technologies in every sense of the word. The disruptive nature refers to the departure from traditional and fashionable techniques and tools.

An observation is necessary here. It is always important to distinguish between the trivial and the non-trivial in science. It is trivial to use existing tools. It is non-trivial to take on the task of developing new tools and instruments. It is trivial to

make generalizations with whatever justifications one prefers. It is non-trivial to employ particular and even singular quantifiers. This concept of the trivial and the non-trivial deserves its own space in areas such as the methodology of scientific research, logic, and the epistemology of science, and of course, includes its applied and experimental derivations.

Three fundamental tools must be mentioned in this same context. All three have to do with measurements.

On one hand, entropy measurement is an important, albeit challenging, issue. As is known, the entropy of a system quantitatively defines the disorder of the system in question. Generally speaking, three approximations are considered chronologically: Boltzmann's, Shannon's, and Zurek's measurements. The first two refer to classical thermodynamics concerning isolated or closed systems. On the other hand, Zurek's measurement addresses the thermodynamics of complex systems. In this context, we must remember that thermodynamics is a unified science that examines isolated systems, in which case entropy is either inevitable or relatively specific. In contrast, in the thermodynamics of complex or even quantum systems, information processes allow for dynamic gradations (Zurek, 1990).

Simultaneously, there is the problem of measuring the uncertainty of a system. More appropriately, it is actually about measuring indeterminacy, for which the necessary referent is W. Heisenberg. And with it, once again, the connection between complexity and quantum. It is simply impossible to measure at the same time the link and direction of any phenomenon, even in the classical world. In the classical world, everything indicates that human beings need security and certainties of all kinds. Indeterminacy is an ontological feature of the Earth itself or the universe. Everything, speaking without further ado, points to the role of chance in the economy of the universe and life.

Well, closely related to the previous measurement, randomness is the third important measurement in the study of non-linear dynamic systems. Thanks to the works of Kolmogorov, Gödel, and Chaitin, there exists a tripartite path in this regard: the first within the framework of mathematics, the second in logic, and the third in computational systems. The close connection among these three areas does not escape a sensitive eye.

Finally, a conspicuous and perfectly distinctive tool of complexity sciences is a unique statistical distribution of complexity: the power law. Originally also called Zipf's law, after its discoverer, the power law appeared in broad daylight thanks to fractal geometry, mainly due to the contributions of Mandelbrot.

A power law is a statistical distribution that works in perfectly different terms: means, medians, averages, trends, vectors, or matrices. Specifically focused on log/log scales, a power law allows us to identify not only various scales and impacts but also what in normal statistics are called *exceptions*; that is, everything outside the parameterizations.

A power law has the merit of clearly identifying the presence of complex dynamics. In other words, whenever the presence or dynamics of a power law is established, it indicates the existence of a complex phenomenon, which encompasses any of the characteristics or attributes previously mentioned in this work.

A power law allows us to identify not only the structure of a system but also its dynamics in comparison to similar or nearby systems—something that other statistical distributions do not offer. The log/log scale refers to the ability to condense a large amount of information (these are logarithmic scales).

More importantly, the study of phenomena, systems, or behaviors that exhibit or are based on a power law shows that, in nature and society, there are phenomena of self-organized criticality (Bak, 1996).

Self-organized criticality aligns well with several aspects of complexity sciences, particularly the study of phenomena far from equilibrium, technically known as punctuated equilibrium, artificial life, and emergent phenomena and properties. This concept is fundamental from an epistemological standpoint and encompasses everything it entails. Complexity exists at the opposite end of causality in any sense of the term. In reality, causality operates only locally and under controlled conditions. However, at meso- and macro-levels and in unregulated situations, causality disappears entirely. Consequently, new semantics, tools, sciences, and disciplines arise, which are specifically those of complexity sciences.

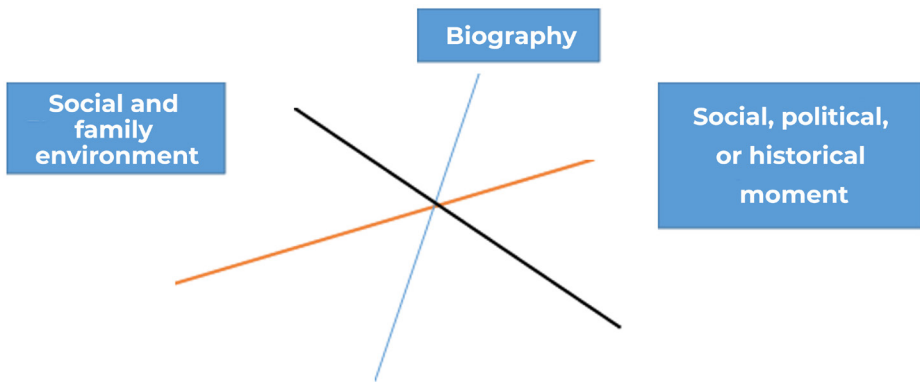
The Internalism vs. Externalism Debate in Science

There is a highly sensitive aspect in understanding science, science and technology, and managing them. This issue is known in the history of science and philosophy as the *debate between internalism and externalism*; that is, the discussion of whether advances in science and technology result from discussions about concepts, tools, experiments, and so on, or whether, additionally and sometimes

mainly, advances or setbacks are also explained by factors external to thought and research, which primarily concern social, economic, cultural, military, or political circumstances. The history of science is prolific in this regard.

A good understanding of what science is in general and how it is possible involves articulating these two aspects, which is easier said than done. Figure 4 illustrates what constitutes a good explanation and triggering of science.

Figure 4. *Defining Lines of Science and Its Management*



Source: Own elaboration.

Figure 4 helps us understand what research is generally, across any field or area of knowledge, how it emerges, and how it becomes possible. The success or failure of an idea, character, or theory results from the interplay of three factors: biography, the social or family environment, and the social, political, or historical moment.

Clearly, the personal experiences of each individual, in the broadest sense (emotions, sexuality, learning, challenges, and opportunities), form the fundamental basis of the research. Similarly, the family and social environment, the education received, foreign language instruction, training in music, and physical skills, for example, provide subtle yet unavoidable insights into each person's intelligence. Furthermore, social or economic events, coups d'état, wars, peace, and social harmony play a crucial role in shaping ideas and intuitions. The examination of the biographies of artists, philosophers, or scientists, along with the analysis of historical periods, societies, and moments, underscores, either explicitly or implicitly, these three fundamental lines.

Then, education, research plans, and public policies would benefit from expanding their observation windows, so to speak, and incorporating a scheme

like the one suggested in Figure 4. These three lines define personal or collective success or failure on any scale and in any context. Herein lies the complexity of the relationship among theory, biography, and the social environment of research, science, and technology.

Understanding cutting-edge science and emerging technologies solely from an internalist perspective is out of the question. A delicate, sensitive, and dynamic balance with externalism is always present, though never obvious.

Thus, two guiding ideas of this work are understood much better: science, in general, always involves democracy, while technology has been, until the birth of the internet, a distinctly military matter. The balance between the military and civil dimensions of life marks essential tensions (Kuhn, 1996) in the complexity of life and knowledge.

In other words, a good understanding of science and technology equates to a broad understanding, experience, and management of dimensions such as psychology, anthropology, health, and aesthetics. These aspects are essential for a comprehensive grasp of science and technology. As can be easily seen, this involves a sensitive and delicate interplay among the humanities, social and human sciences, and the sciences and engineering.

Approach to Cyberspace and Cyber Defense

Security and defense issues primarily refer to themes, dynamics, problems, and actions amid uncertainty, to essentially unpredictable phenomena, to a significant capacity for improvisation and rapid learning, and finally, to non-linear dynamics in the full sense of the term.

I want to maintain that the issues of security and defense refer to much more than merely the defense of institutions, territory, life, and nature itself. Thus, any State must deeply understand the best of cutting-edge research, collaborate on it, and contribute to its dissemination.

Politically and legally, institutions do not owe a duty to the State or the republic but to the nation. They have a duty to the people, the territory, and the protection and defense of nature. Institutions are merely means, tools, or instruments to an end: the defense, care, exaltation, enabling, and gratification of life. Human life, as well as life in general, exists within the framework of national geography. And often, it extends beyond geography.

Manifestly, the above indications are far from commonplace in an institutionalized atmosphere in the world. I am referring explicitly to institutionalism and neo-institutionalism.

We find ourselves, both nationally and globally, within the framework of fifth-generation wars. This situation arises from a social and cultural phenomenon unprecedented in the history of humanity. It concerns the transition from the analog world and society to their digital counterparts.

We live in a world today that is immensely rich—rich in data. There are no longer, nor is it possible to speak of, variables in any sense of the word. A figure, a gesture, a letter, a movement, a relationship, a name, for example, are data. And the data are understood in the context of informational and computational systems. Life, in general, is impossible with your back turned to computing.

As is well known, the internet is composed of superficial information—as in the famous iceberg analogy—and the information that exists on the deep web, which constitutes, by far, the majority.

Today, intelligence, *lato sensu*, encompasses knowledge of informational and computational systems, as well as navigating the internet. To be more specific: Human intelligence today fundamentally involves developing or acquiring a hacker mentality. The best companies, universities, and corporations now recognize the importance of including in their governing bodies not just the vice president of marketing, the head of logistics, the manager of general personnel, and others, but also a hacker, who has two main functions: first, to prevent the hacking of the company, organization, or institution, and second, to hack the competition.

Cyber defense, broadly speaking, concerns not only state or governmental dimensions but also industrial, business, and knowledge aspects. Knowledge is an organization's true asset; it represents the know-how and literally costs a fortune.

In the past, espionage was primarily military. Today, it also encompasses civil, industrial, and other forms. This notion suggests a fundamental acknowledgment.

Information is weightless; it can be kept as long as necessary, accumulated in various ways, and compartmentalized as needed. Likewise, information can be shared without losing it. You can always use it for any purpose, whenever you want. All of this points to the importance of the digital footprint. (Let us say in parentheses that the digital footprint is indelible, but it can be hidden, which requires technical knowledge of computing and information.)

Contrary to all appearances, the most essential things happen primarily in cyberspace, which is precisely the space of the digitalization of the world and reality.

As already mentioned and acknowledged, most information is found on the deep web. If UNESCO has rightly pointed out that currently, the main form of illiteracy is technological illiteracy, the vast majority of citizens and their organizations, of all kinds, remain functionally illiterate due, among other reasons, to their ignorance in browsing the deep web. Open data policies, as well as open science policies, fundamentally pass through this area.

Complexity sciences know this, work on it, and deploy research capabilities.

There are numerous works on complexity and military topics, and the research centers worldwide on these two lines are robust. Additionally, some journals specialize in this subject. Even adversaries recognize the significance of complexity sciences, *lato sensu*, when addressing critical issues such as democracy, freedom, national interest, geostrategic positioning, control, security, defense, and attack, along with all their derivations and intertexts. This is not the focus of this chapter, simply due to space limitations. A solid state-of-the-art, which, if the expression fits, represents the ABC of good research, thus highlights it well.

In any case, it is evident that as information is deposited in digital form, it is both secured and exposed, however paradoxical it may seem. The topics that arise then are encryption, cryptography, decoding, and coding, all of which refer to the interface between quantum and complexity (Maldonado, 2010).

Cyberspace is the world of cryptography today. Currently, the battle, so to speak, is being won by the *encryptors*—an exciting topic is quantum cryptography. However, with the development of quantum computing, the relationship will reverse in favor of *decryptors*, regardless of the technicalities used by the former, one of the most reliable being the work with the Riemann zeta function.

Cyber defense, cyberspace, and issues related to cybersecurity run cross-cuttingly, as shown in Figure 1 above.

Conclusions

We are witnessing a magnificent development of science and engineering like never before in the history of humanity. The most important task for all those who, in some way, revolve around knowledge—that is, knowledge, information, education, culture in a broad sense, research—is to stay up to date, as much as possible, with the state-of-the-art. The difficulty lies in the rhythms and interconnections of these developments. Fortunately, there are numerous channels available for this.

Just one example: the briefings from Nature—one of the most influential journals in the world—that we may receive every day.

I want to emphasize this: the best cutting-edge research in the world is rooted in the complexity sciences. Just look at the most significant think tanks, broadly speaking, around the globe.

Stated negatively, complexity sciences address everything that traditional science overlooks; for instance, irregular movements, uncertainty, indeterminacy, unpredictability, sudden and unforeseen changes, irreversible alterations, the breakdown of balances and control, and the possibilities, even the impossibilities, of the real, or what remains beyond the parameterizations. This list could easily be expanded.

To achieve this, sciences have deployed a dual apparatus: one conceptual and the other instrumental. However, both are fundamentally the same. The distinction is purely analytical.

From any point of view, today, good intelligence consists of the articulation of two parallel and complementary levels: human intelligence and technical intelligence. The best expression of the latter is artificial intelligence. The best expression of the former... what it consists of still needs to be clarified.

Artificial intelligence forms one of the best sedimentations of complexity sciences (Maldonado, 2023b). Table 1 specifies this idea.

Table 1. Relationships between Artificial Intelligence and Artificial Life

ARTIFICIAL INTELLIGENCE	ARTIFICIAL LIFE
Turing Test: Distinguishing the human mind from the machine	Understanding life through computing
Different types of TM (Turing Machine)	Games: Earth, The Game of Life, etc.
Associativism vs. connectionism	Genetic algorithms
Neural networks	<i>Bottom-up</i>
Top-Down	

Source: Own elaboration.

The idea that follows from Table 1 is relatively easy. Artificial intelligence (AI) and artificial life (AL) are the same despite their origins in different frameworks and times.

Thus, the topics and problems of cyberspace and cyber defense are well understood based on AI/AL. Everything else is simply operational.

These are turbulent and fluctuating times, characterized by uncertain and unstable dynamics. In short, they represent chaotic circumstances and relationships that demand new and improved tools of all kinds, theoretical or conceptual, as well as the best possible or imaginable technology. The challenges and problems stimulate our intelligence, rather than voluntaristic purposes or ideas, regardless of how well-intentioned they may be. In this context, intelligence is simply the term we use to describe the key to accessing learning and adaptation, if such a metaphor is possible.

Let us conclude with a subtle analogy. Complexity sciences represent a scientific revolution. They are, simply put, still considered an alternative science. The reason is not difficult to understand and is much better illustrated by medicine or biology. When confronted with a new, foreign body, every organism instinctively closes itself off and rejects it. The organism seeks to preserve itself; in principle, any new entity poses a threat. However, the true danger lies not with the new body but with the organism itself, which may lack the intelligence necessary to maintain homeostasis. The body fails to recognize that it cannot heal and recover without significantly modifying its metabolism. That is what life entails: metabolic processes and networks. And yes, it is possible to transform and change your metabolism. What is at stake is health and life.

References

- Bak, P. (1996). How nature works: *The science of self-organized criticality*. Springer Verlag.
- Camazine, S., Deneubourg, J.-L., Franks, N. R., Sneyd, J., Theraulaz, G., & Bonabeau, E., (2003). *Self-organization in biological systems*. Princeton University Press.
- Gray, J. J. (2003). *El reto de Hilbert: Los 23 problemas que desafiaron a la matemática*. Crítica.
- Kuhn, T. (1996). *La tensión esencial: Estudios selectos sobre la tradición y el cambio en el ámbito de la ciencia*. Fondo de Cultura Económica.
- Maldonado, C. E. (2010). Una nota sobre criptología y complejidad: Un caso de complejidad y administración. *Innovar*, 20(38), 5-12. <https://revistas.unal.edu.co/index.php/innovar/article/view/22280/23192>
- Maldonado, C. E. (2013). Un problema fundamental en la investigación: Los problemas P vs. NP. *Revista Logos Ciencia & Tecnología*, 4(2), 10-20. <https://doi.org/10.22335/rclct.v4i2.186>
- Maldonado, C. E. (2019a). Sociedad de la información, políticas de información y resistencias: Complejidad, internet, la red Echelon, la ciencia de la información. Desde Abajo.
- Maldonado, C. E. (2019b). Quantum Theory and the social sciences. *Momento*, (59E), 34-47; <https://revistas.unal.edu.co/index.php/momento/article/view/81645/0>
- Maldonado, C. E. (2020a). *Camino a la complejidad: Revoluciones científicas e industriales: Investigación en complejidad*. Asociación Rujotay Na'oj.
- Maldonado, C. E. (2020b). *Pensar: Lógicas no-clásicas* (2nd ed.). Universidad El Bosque.
- Maldonado, C. E. (2021). Epistemología de la imposibilidad o ciencia de la indeterminación. *Cinta de Moebio*, (70), 44-54. <https://cintademoebio.uchile.cl/index.php/CDM/article/view/61586>
- Maldonado, C. E. (2022). Teoría de los problemas complejos. *Cinta de Moebio*, (74), 109-120. <https://doi.org/10.4067/S0717-554X2022000200109>
- Maldonado, C. E. (2023a). A systemic problem cannot be solved systemically. *Cinta de Moebio*, (77), 79-88. <https://doi.org/10.4067/S0717-554X2023000200079>
- Maldonado, C. E. (2023b). *Inteligencia artificial y ética*. Desde Abajo.
- Maldonado, C. E., & Gómez-Cruz, N. (2011). *El mundo de las ciencias de la complejidad*. Universidad del Rosario.
- Pagels, H. (1991). *Los sueños de la razón: El ordenador y los nuevos horizontes de las ciencias de la complejidad*. Gedisa.
- Prigogine, I. (2003). *Is future given?* World Scientific.
- Zurek, W. H. (Ed.). (1990). *Complexity, entropy, and the physics of information*: CRC Press.

Chapter 5

Power in the Information Age: Perspectives on Cyber Power*

DOI: <https://doi.org/10.25062/9786287818064.05>

Milena Elizabeth Realpe Díaz

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: This chapter analyzes the dynamics that take place in cyberspace. It explains how cyber power is beginning to be discussed in the general sphere of power while examining the meanings of the term according to different regional perspectives. It also describes the power from the U.S. military and the European Union perspectives. It expands the understanding of cyber power based on its location, all of which aim to establish adequate estimates of this subject matter.

Keywords: cyber conflict; cyberspace; cyber power; cybersecurity; power

* 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

Milena Elizabeth Realpe Díaz

Lieutenant Colonel of the Colombian National Army. PhD candidate in Strategic Studies, Security and Defense, and Master's in Cybersecurity and Cyber Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. Master's in Information Security, Universidad de los Andes, Colombia. Specialization in Computer Network Security, Universidad Católica de Colombia. Specialization in Physical and Computer Security, Escuela de Comunicaciones del Ejército, Colombia. Specialization in Information Security, Universidad de los Andes. Bachelor's in Systems Engineering, Universidad Cooperativa de Colombia. Head of the Master's in Cybersecurity and Cyber Defense, Escuela Superior de Guerra "General Rafael Reyes Prieto," Colombia. <https://orcid.org/0000-0003-4345-6182> - Contacto: milena.realpe@esdeg.edu.co

APA Citation: Realpe Díaz, M. E. (2025). Power in the Information Age: Perspectives on Cyber Power. In M. E. Realpe Díaz, & A. M. González González (Eds.), *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* (pp. 129-150). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818064.05>

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

The technological revolution in the last years of the 20th century profoundly impacted how people relate to each other and perceive the world around them. The arrival of the internet and the digitization of information revolutionized the transmission and processing of information. For its part, the information technology revolution reshaped the material bases of a new society. Information technologies have become indispensable tools for generating wealth, exercising power, and creating cultural codes (López, 2002). According to Castells, this period of technological revolution corresponds to a historical interval during which the advances achieved by information technologies changed society's material culture, significantly influencing various activities performed by individuals, not as an exogenous source of impact but as a direct one (Castells, 2001, p. 112).

Additionally, the development and implementation of technologies have caused an accelerated transformation of the material base of society, profoundly affecting how people relate to one another and perceive the world around them, giving rise to the *information society*. This signifies that these technologies are present in people's daily lives and are used across various activities, from work and education to entertainment and interpersonal communication. As Estudillo states, it is a society in which new technologies and information affect the social structure in different areas of human life, such as the economy and social well-being (2002, pp. 83–84). Likewise, Castells (1996) maintains that information and communication technologies (ICT) are the driving force behind the transformation of society and have enabled the creation of a global economy and the real-time connection of people worldwide.

As Perlroth (2022) states, the internet, like many other things we now realize, has left us inextricably connected. Digital vulnerabilities that affect one affect all.

The barrier between the physical and the digital is increasingly insignificant. It is true that everything "can be intercepted," and most of what matters to us has already been intercepted: our personal data, intellectual property, chemical companies, nuclear power plants, and even the country's cyber weapons (p. 475). With this perception, technological progress and the internet are viewed as factors of social change. In this context, as noted by De Vergara and Trama (2017), the internet and technological developments have also significantly influenced the character of wars and conflicts. Several 21st-century authors agree, reiterating Clausewitz's postulates that conflicts are like a chameleon, changing their character depending on their nature, purpose, how they are led, the technology used, and the operational environment in which they occur (p. 58).

Thus, cyberspace arises as the common scenario where social, commercial, industrial, technological, and military interactions occur among people, organizations, institutions, banks, and armies. In this realm, threats, both criminal and those aimed at destabilizing states, often connect to rival or enemy countries. These actions result in cyber conflicts, "a type of conflict that takes place in cyberspace and that can involve military, intelligence, propaganda, and sabotage operations, in which actors use cyber tools and techniques to achieve their objectives" (Singer & Friedman, 2021, p. 2). An escalation of such hostilities in cyberspace leads to a cyber war, "...a serious form of disruptive cyber attack by a nation on another nation's cyberspace, crossing the line into being considered a use of force. Issues of the Law of War come into play" (Hunker, 2010, p. 4). In this context, a new concept emerges: *cyber power*, defined as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power" (Kuehl, 2009, p. 25).

As defined by Mitchell (1995), cyberspace is a new, digital dimension without borders, a space for communication and information exchange that has become an integral part of the daily lives of many people. It is a reality where new technologies bring opportunities and vulnerabilities for the most developed countries while contributing to an increasing technological gap with developing countries, especially concerning national security and defense (Ferreira, 2018, p. 36).

While technology has brought numerous benefits, it has also raised new ethical, political, and legal challenges that are still being addressed. If the multiple sources of information are analyzed, technology is becoming more accessible every day, allowing new threats to emerge from illegitimate regimes, terrorist groups, organizations outside the law, and organized crime that may have access

to cyberterrorism, cybercrime, weapons of mass destruction, arms trafficking, and more. This implies a change in the concept of the traditional threat posed by identified enemies (CESEDEN, 2012, p. 126).

The above shows great concern, not only national but international, because although the relationship between the information society and cyberspace has brought significant benefits in terms of communication and globalization, it has also created a series of risks and challenges for society. It is important that steps are taken to address these issues and ensure that the benefits of technology are used responsibly and equitably.

From Power to Cyber Power

Historically, it was believed that a country's power depended on aspects such as its geographical location, national resources, the number of inhabitants, and its wealth, as these were considered essential elements for the development of military strength (Tellis et al., 2009). Traditionally, a country's ability to safeguard its borders from potential attacks, while being capable of threatening neighboring nations, was perceived as the ultimate symbol of its national strength. However, with the transition to the Fourth Industrial Revolution, conceptions of national power have evolved, incorporating the notion of a knowledge revolution. This transformation signals a significant change in the importance assigned to information technology and innovation within the structure and dynamics of society.

The evolution of the conception of power, from traditional notions based on geographical and economic factors to a new paradigm of cyber power, reflects the necessary adaptation to the Fourth Industrial Revolution. In this transition, the relevance of information technology and digital interconnection becomes a crucial element. The ability to leverage cyberspace to achieve strategic and tactical objectives redefines the landscape of influence and security in both national and international contexts. As digital technologies continue to evolve, it is imperative to address this emerging dimension of power in the contemporary era, where technology and information play a central role in shaping power dynamics and global relationships.

Migrating from power to cyber power implies adopting a series of measures and strategies that enable the utilization of the capabilities and resources of cyberspace to achieve strategic and tactical objectives. Additionally, it requires a significant transformation in how nations, organizations, and individual actors influence the global stage. This is due to the growing importance of information,

communications, and operating technologies, as well as interconnection through the internet (Kuehl, 2009). The transition from a conventional power structure to a cyber power paradigm signifies the increasing preeminence of digital technologies and cyberspace in shaping influence and security in both national and international contexts. As these technologies continue to evolve, analysis and adaptation to this emerging dimension of power in the contemporary era become imperative.

In summary, traditional power and cyber power are two concepts that are intertwined today. On one hand, all power can be characterized as “the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances and fate” and is only made evident by the effects it has on others (Barnett & Duvall, 2005). On the other hand, cyber power can be understood as the variety of powers that circulate in cyberspace and shape the experiences of those who act in and through cyberspace (Jordan, 1999, p. 3). Cyber power “is not created simply to exist, but rather to support the attainment of larger objectives... across the elements of national power—political, diplomatic, informational, military and economic” (Kuehl, 2009, pp. 41–42). Cyber power is one of the latest additions to the family tree of power, given how recent the digitalization of our societies and the emergence of cyberspace still is.

From Cyberspace to Cyber Power

To trace the evolution of cyberspace, from its origins to contemporary society, it is necessary to mention that this scenario is considered a strategic domain due to its capacity to transform society, influence the economy and politics, and affect the security and defense of countries. On this premise, it is essential to recognize that *cyberspace* is a term that has been used for approximately half a century; therefore, it is natural to present its evolution. This was first introduced in the book *Future Shock*, by Alvin Toffler (1970). Later, it was used and recreated by William Gibson in his works *Burning Chrome* (1982) and *Neuromancer* (1984), and consequently, it has multiple definitions, such as the one established by Bauman (2000): cyberspace is a space of uncertainty and ambiguity, where social identities and relationships can be easily constructed and deconstructed. For Castells (2010), cyberspace is a virtual space that extends beyond the physical world, in which users can interact, collaborate, create, and share information and knowledge, and in which information and communications technology play a central role (p. 69).

The history of humanity is also a record of the constant confrontations between civilizations and peoples. Modernity, for its part, brought with it two world wars, possibly the bloodiest known to date; however, it must be acknowledged that these gave rise to various formal institutionalized initiatives, such as the UN, along with a significant number of theoretical approaches that, for example, revitalized the romantic Kantian idea of perpetual peace (Kant, 1795), or defined or reinforced the notions and necessity of adhering to human rights (HR), International Humanitarian Law (IHL), and the traditional laws of war (LOW), which divide the *Jus ad Bellum* (the decision and causes of starting the war) from the *Jus in Bello* (which regulates the conduct of war).

Kant's idea was romantic and even anachronistic, yet materially correct, as the creation of a league of nations was a plausible initiative. Even though its operational ineffectiveness or the emergence of new forms of conflict and oppression at its expense would later be seen under the banner of humanitarian intervention or peace operations, Fisher (2011) points out that humanitarian interventions can take a wide variety of forms, from the provision of aid to the use of military force (p. 221). It is essential to quote Kant to contrast good ideas and intentions with pragmatic political achievements, along with their results and impacts.

Preliminary articles of perpetual peace between states. 2) No state having an independent existence—whether it be great or small—shall be acquired by another through inheritance, exchange, purchase or donation. 3) Standing armies (*miles perpetuus*) shall be abolished in course of time. 5) No state shall violently interfere with the constitution and administration of another. (Kant, 1795, pp. 247-249)

We will leave this reflection at this point only to note that the regulations of war and human conflicts evidently fall short and are inappropriate to meet the demands of cyber conflicts, which are even more complex, diffuse, and conditioned.

The *postmodern global order*, as it is appropriate to call it, is usually studied from international relations, science, and political philosophy. For Gómez (2017), it is analyzed in terms of structure, actors, processes, their relationships, power, and phenomena such as violence. The structure is determined by the inclination toward the ordered or anarchic model of the international system; the position of the actors depends on the roles they play; and the processes operate based on interactions of conflict or cooperation (p. 59).

According to Hardt and Negri (2004):

In the contemporary global order, a permanent global war is waged where the actors, even without pursuing common objectives and despite their inequalities, must cooperate [...] Empire rules over a global order that is not only fractured by internal divisions and hierarchies but also plagued by perpetual war. The state of war is inevitable in Empire [...] War is becoming a general phenomenon, global and interminable [...] a general global state of war that erodes the distinction between war and peace such that we cannot longer imagine or even hope for a real peace [...] the traditional distinction between war and politics becomes increasingly blurred [...] war, that is to say, is becoming the primary organizing principle of society, and politics merely one of its means or guises. (p. 8)

What stands out about Hardt and Negri's approach to the contemporary global order is that the very notion of *world power* has eroded. While it is true that there are key actors who fight tirelessly for economic hegemony, like China, or geostrategic hegemony, like Russia, complex interdependencies and the need for vital resources and dispersed interests make cooperation, deterrence, or even deception valid strategies for prospering and gaining advantage. This is especially relevant since many of these assets are intangible, products of knowledge, software, and cyber weapons available to the highest bidder, free from the control of states. This is reflected in Nicole Perlroth's research recorded in her book, *This Is How They Tell Me the World Ends*:

For decades, under the protection of classification levels and confidentiality agreements, the U.S. government became the world's leading zero-day hoarder. U.S. government agents paid a high price (first thousands, then millions of dollars) to hackers willing to sell their lock-picking codes and their silence. But then, the USA lost control of its supply and the market. Now those zero-days are in the hands of hostile nations and mercenaries who do not care if your vote is lost, your water is polluted, or our nuclear power plants collapse. (Pelroth, 2022, p.1)

Studying cyberspace power helps us understand current threats. In an increasingly digitalized world, military operations and national security depend heavily on cyberspace systems. Grasping their importance will provide a clear path to protecting national interests, maintaining international stability, and promoting scientific and technological progress in the field of cybersecurity.

Foucault (1966) states that scientific knowledge is linked to power relations and that scientific discourse can be used to justify forms of social domination. Studying cyberspace power is essential because cyberspace has become a fundamental component of modern military activities. In this context, current military conflicts often involve cyber operations, which can significantly impact a country's ability to protect itself or conduct military operations.

In contexts of war, as well as in scenarios where it has not been explicitly declared, as Hardt and Negri would affirm, within the scope of permanent global war, various types of incidents are emerging in cyberspace—attacks or conflicts that illustrate the competition for power among different states, corporations, or national and international organizations. Valeriano and Maness assert that, in cyberspace, competition for power and influence is central to cybersecurity and cyber conflict. This approach carries significant implications for international politics and security, as cyberspace evolves into a new domain of strategic competition within the international system (Valeriano & Maness, 2015).

It is time to say that, based on the premise of permanent global war, ways of waging it have emerged that have led to definitions such as fifth generation wars, hybrid wars, cyber wars or cyberconflicts, and the special war doctrinally developed by the U.S. Army in the U.S. Army Special Operations Manual, ADP 3-05 (2012, p. 9), as well as MDOs (multi-domain operations). They all share the commonality of being carried out, using, or involving actions in cyberspace to a greater or lesser extent; consequently, understanding them is essential when assessing the cyberspace power related to each of them.

Many actions occur in cyberspace; moreover, it can be asserted without hesitation that these actions are executed by state actors, intelligence forces, and agencies. Media and cyberspace operations are conducted, often undisclosed, of which we can only observe the effects. For our topic, this is, *a priori*, unapproachable or even ineffective, but in reality, it is precisely the foundation of our inquiry. What types of cyber weapons are utilized? How do they function? How significant is the role of artificial intelligence in all this? And what is of utmost interest: How, being clandestine, can these capabilities be assessed as part of a State's arsenal or cyber power?

Hybrid wars, according to the LISA Institute, are those that combine military force with elements such as cyberattacks, manipulation of information via the internet and social media, or economic pressure. In such wars, cyberspace serves two functions: as a tool for conducting information operations and related

actions, or as a battlefield where specific adversarial objectives are pursued. In this scenario, the use of cyber weapons is extensive, and their application is typically more evident and regulated, even doctrinally, as operations in cyberspace; case studies will be extremely useful in determining the extent of this regulation.

Before addressing cyber conflicts, the so-called special warfare is introduced. It is defined by the RAND corporation (2016) as a peculiar form of war and a strategy to protect and achieve U.S. national interests from a realist perspective that pays little attention to the ethical implications of the procedures. This approach is considered justified and permissible for intervening in other countries indirectly or surreptitiously, taking advantage to benefit unilateral interests while avoiding the compromise of troops and resources in decisive confrontations (p. III).

In many cases, special warfare can be viewed as a non-obvious war. According to Libicki (2012), technological and organizational innovations in recent decades have created the potential for a non-obvious war, where the identity of the fighting side and even the mere fact of war are completely ambiguous (p. 19). Libicki (2012) further points out that technological attacks—cyber warfare, space warfare, electronic warfare, drone warfare—and other strategies with long historical antecedents, such as sabotage, assassination, and the use of mines, are part of the spectrum of actions that can be executed in a non-obvious way. In all these cases, ambiguity underlies the lack of evidence: while the actor remains unknown, the act does not. Some non-obvious incidents of war would clearly be considered acts of war if they were more evident (p. 19).

It is indisputable, and we reaffirm it once again. In the study of cyber power, this form of warfare complicates the assessment and estimation of a state's actual assets and resources, as well as those it pays to enable these questionable ends.

In this type of warfare, political differences and global power dynamics are manifested through economic, military, and informational actions that impact the civilian population. This creates a breeding ground exploited by various global actors to enhance their power in cyberspace as an operational field. This includes not only strategic objectives targeting critical cyber and information infrastructures but also utilizing cyberspace as a repository of information where cyber and cognitive operations are consolidated as the fundamental source of hybrid conflict (Cano, 2021). The above highlights the importance of cyberspace today and how its evolution can affect the security, stability, and development of nations.

The President and founder of the World Economic Forum, Klaus Schwab, and author of the book *The Fourth Industrial Revolution* (Schwab, 2017), states that

the Fourth Industrial Revolution promises great social changes. This technological revolution will completely alter the products we make, how we make them, how we interact, and, above all, who we are. As expected, this potential, characterized by the promise of automation and the interconnection of physical ecosystems with digital ones (Internet of Things, neural implants, smart prostheses, etc.), will not only offer benefits but will also pose dangers. War will also undergo changes (p. 2).

Schwab's aforementioned words present us with a form of conflict that is even more complex, where threats may not originate from actors in another country yet can endanger the strategic assets of states. This situation involves overwhelming threats in the face of which, without a doubt, traditional responses will be ineffective. Virtually, a redefined and possibly non-existent cyberspace military power will be required in the majority of the globe's defense forces.

From a strategic perspective, cyberspace has been recognized as an area of strategic importance for military power by many authors and organizations. In this context, Castells points out that cyberspace is a domain of global power with the potential to transform the functioning of society and the State. According to the author, digital networks enable the creation of new forms of political, economic, and social organization that can challenge the authority of traditional institutions (Castells, 2001). Furthermore, Kramer (2009) argues that cyberspace is a fundamental dimension of cyber power and national security, as conflicts in cyberspace can have devastating consequences for the critical infrastructure of countries and for the security of citizens. In modern society, cyberspace has become an essential arena for political, economic, and military activity, along with the role that artificial intelligence and cyber defense play in managing cyber conflicts (Arellano, 2019). In this regard, Psychogiou (2022) establishes that cyberspace has become the fifth battle space in an increasingly complex security landscape, and cyber threats have become part of the purview of international security (p. 1).

The above demonstrates that cyberspace has become a fundamental tool for the functioning of modern societies. Countries that can control and dominate cyberspace gain a significant advantage in military, economic, and political spheres. Cyberspace has transformed into a battlefield where nations can conduct covert operations without direct military intervention, enabling them to achieve strategic objectives without facing the consequences of armed conflict. Consequently, a relatively new form of conflict arises: *cyber conflict*, which becomes increasingly relevant as dependence on technology and the global interconnection of information systems grows.

Cyber conflicts should be regarded as a threat to national security and defense because cyberspace has become an essential dimension of the economic, political, and social life of nations—a virtual environment where communication activities and information exchanges occur through interconnected networks, technologies, and people. Incidentally, Thomas Rid (2012) has defined cyber conflict as the use of cyber means to trigger, escalate, or prolong a real-world armed conflict. Carr and Tikk (2021) argue that cyber conflict is a conflict involving the use of cyber tools and techniques to inflict damage or disrupt the computer systems of adversaries, which can have significant consequences for security, politics, and economics (p. 6). Additionally, Singer and Friedman state that cyber conflict is “a type of conflict that takes place in cyberspace and that can involve military, intelligence, propaganda, and sabotage operations, in which actors use cyber tools and techniques to achieve their objectives” (Singer & Friedman, 2021, p. 2). Although the definitions studied present a broad spectrum of perspectives on the subject, they all agree that cyber conflict entails the use of information and operational technologies to conduct hostile actions in cyberspace, either to damage or disrupt adversaries’ technological systems or to achieve political, military, economic, or other objectives.

Meanwhile, Alberts and Hayes (2003) argue that cyber conflicts have become a significant threat to national security since computer and communications systems are essential for the functioning of the economy, government, and defense. The authors warn that cyberattacks can have serious consequences for critical infrastructure and society as a whole. Today, the nature of warfare and security has changed with the evolution of technology and the emergence of cyberspace as a new battlefield, presenting unique challenges and requiring a multidisciplinary approach. Various authors have addressed the importance of studying cyber conflicts. For example, Kramer argues that cybersecurity is fundamental to national security and that states must consider the technological, political, and social aspects of cyber conflicts. For his part, Libicki discusses the concept of cyber deterrence and the threats involved, highlighting how retaliation can help deter cybercriminals. Cyber conflicts are an expression of power in the information society, where the control of information and technology is essential (Libicki, 2018).

As noted, one of the challenges for studying cyber power, which also exhibits a notable strategic advantage of cyber conflicts, is that these can be carried out covertly, without the need for a large investment of material and financial resources and with the possibility of causing a great impact on the critical infrastructure of

a country or an organization. Additionally, cyberattacks can be launched from anywhere in the world, making it difficult to attribute responsibility to a specific actor. Clarke (2010) argues that cyberspace offers a strategic advantage to adversaries because it allows them to operate undetected and affect critical systems such as infrastructure, communications networks, and military systems. This new form of conflict allows state and non-state actors to level the playing field against stronger adversaries, considering that cyberspace is a domain in which size and economic capacity are not necessarily determinants for the success of an attack. Kramer argues that cyber conflict can provide actors with a tactical advantage by allowing them to penetrate adversaries' information and communication systems to obtain classified information or disrupt command and control systems (Kramer, 2009).

Another strategic advantage of cyber conflicts is their ability to inflict damage and impact key objectives without the need for a conventional military force. Through cyberattacks, they can cause significant harm to critical infrastructure systems, such as energy, transportation, healthcare, and finance, which can have serious repercussions for the economy and society as a whole. According to Rid (2013), cyber conflicts allow powerful actors to extend their influence into cyberspace without the costs associated with conventional military operations (p. 4). This enables them to inflict considerable damage on critical infrastructure systems, financial and communications networks, among others, without putting their own military forces at risk. Cyberattacks can serve as a form of coercion and deterrence in international relations, conveying messages to other global actors and threatening greater repercussions if certain conditions are met (Libicki, 2009, pp. 11–12). Fernández (2022) states that from 2021 to the present, cyberattacks have been utilized as a non-conventional weapon among States; the primary parties involved have continued to be the nations that previously demonstrated significant activity in cyberspace, namely the USA, China, Russia, and the European Union, which are now joined by other countries that have previously not been very active in cyber conflicts, such as India, as well as other consistently active players like North Korea, Israel, or Iran (pp. 313–314).

From these statements, one can infer that the strategic advantage of cyber conflict lies in its capacity to inflict significant damage without risking one's own military forces. Additionally, it serves as a tool for coercion and deterrence in international relations. Cyberspace military power represents a latent priority on countries' agendas; however, we must not overlook the fact that this reality complicates how nation-states define, value, and acquire their cyberspace military power.

Cyber power is a form of power projection in the information age, and its development is essential for the security and defense of nations. Sánchez (2019) argues that cyberspace power is a critical tool for national security and defense, as it allows states to protect their critical computer systems and ensure their sovereignty in cyberspace. The author contends that cyber power is an integral component of national security and that its development should be a priority for governments. According to Segal (2017), cyberspace power refers to the ability to control and exploit cyberspace to achieve political, economic, or military objectives, whether by protecting one's own critical infrastructure or disrupting that of adversaries.

Cyber power allows us to achieve superiority or supremacy in cyberspace. This capability can provide a country with a strategic advantage regarding national security, politics, economy, and military. By establishing strong dominance in cyberspace, a country can protect its own information and communication systems while simultaneously spying on, sabotaging, or disrupting other nations' systems. Furthermore, cyberspace serves as a crucial platform for the digital economy and technological innovation, meaning that a country with an edge in cyberspace can secure a leading position in global trade and technology. Therefore, the contest for superiority or supremacy in cyberspace has become an important aspect of today's geopolitical competition. Countries strive for dominance in cyberspace because they believe that controlling information and communications in this domain is vital for their security, economy, and global influence. The competition for superiority in cyberspace significantly impacts national security and international relations (Sanger, 2018).

Countries compete for superiority in cyberspace to maintain national security, protect economic interests, and ensure political and social stability (Tikk & Kerttunen, 2020). They strive for this superiority because information and knowledge are the most valuable resources in the world today, and controlling these resources is key to power and influence (Stavridis & Farkas, 2012). This reflects the necessity for a nation or organization to develop cyber power and assert its superiority or supremacy.

Cyber power has become a fundamental element for national security and the defense of States because cyberattacks can cause serious damage to critical infrastructure and the economy of countries (Cujabante et al., 2020; Libicki, 2018; Valeriano & Maness, 2020).

Perspectives on Cyber Power

According to Nye (2011), not only have the types and sources of power in countries changed, but these changes also occur in the international context, specifically the scenario where States coexist. It is important to note that countries must coexist with other non-governmental actors. The perspectives on cyber power are broad and varied. First, cyber power is viewed as an essential tool for power projection in the modern world. Unlike traditional power, which is based on physical force and coercion, cyber power relies on the ability to influence and control individual behavior through cyberspace. Although cyberspace has not yet been used as a medium to exhibit the conventional hard power of coercion and threats supported by physical force, it does offer a suitable platform for projecting the soft power of attraction and imitation. Finally, the perspectives on cyber power are presented and analyzed from American military or strategic viewpoints (Kuehl, 2009; Nye, 2010) in contrast to Dunn's (2018) interpretations regarding cyber power in the European Union.

To continue this analysis, it is necessary to understand what I have termed the *localization of cyber power*, which follows two trends: the first is linked to the definitions of military cyber power and corresponds to a reductionist perspective that views cyberspace as a management tool that must be preserved to maintain the initiative; hence, operational efforts focus on generating protocols for the defense of strategic assets, sometimes pertaining not to the nation but to the forces, which is even more limiting. The other perspective, referred to as *comprehensive*, is expressed with the definition of cyber strategy or cyber power integrated into other domains or forms of national power; it incorporates and expands the core and capabilities associated with cyber power, based exclusively on the cyberspace domain, and adds or integrates with other components.

Cyber Power in the USA

To understand cyber power from the theory of military cyber power proposed by Gaines (2015), it is necessary to understand the terms and principles that form the basis of this theory and help to understand and apply operations in cyberspace in the context of joint operations and the expansion of combat power:

- Cyberspace: A global domain that encompasses physical, logical, and personal elements in the cyber realm.

- Cyber power: The application of operational concepts, strategies, and functions that employ operations in cyberspace to enhance combat power and achieve military objectives.
- Cyber military strategy: The development and employment of operational capabilities in cyberspace, integrated with other capabilities across different domains, to expand combat power and reach military objectives.
- Key terrain in cyberspace: Any physical, logical, or personal element of cyberspace that, if disrupted, degraded, or destroyed, limits combat power and provides a significant advantage to one of the combatants.
- Military cyberspaces: The various cyberspaces that exist, considering their diversity and heterogeneity.

Based on these precepts, the theory proposed by Gaines states that the integration of cyberspace operations with joint operations can expand joint combat power in several ways (Kern, 2015).

Operations in cyberspace present a series of strategic advantages. First, they offer greater attack capability, enabling joint forces to disrupt the enemy's command and communication infrastructure, significantly weakening their ability to respond. Additionally, these operations provide enhanced defense, allowing joint forces to safeguard their own networks and systems against cyberattacks, thereby ensuring the integrity of their combat power. Cyber operations offer greater situational awareness by gathering real-time information on enemy activities and capabilities, which facilitates informed decision-making and agile adaptation to changing situations (DoD, 2011).

Finally, these operations can support and enhance other military capabilities, such as land, sea, and air operations. This translates into increased effectiveness and coordination in joint missions, either by neutralizing enemy defenses before a conventional attack or by providing intelligence and communications support during combined operations. Overall, integrating cyberspace operations into joint operations expands combat power by introducing new forms of attack and defense, improving situational awareness, and leveraging additional military capabilities (Gaines, 2015).

Cyber Power in the European Union

Driven by ongoing concerns about threats from cyberspace, cybersecurity has emerged as a priority issue on the political agendas of States and international and supranational organizations, including the European Union (EU). The associated

policy debate centers on measures to regulate behavior in cyberspace, aiming to transform it from a rebellious and insecure environment into a more stable, reliable, and orderly one. At the heart of this discussion are fundamental questions of power and control (Dunn, 2018).

The difficulty with the concept of cyber power is that there are still no systematic (empirical) analyses of the topic; in fact, the body of literature on cyber power is small and fragmented. Existing texts, including those specifically addressing European cyber power (Klimburg & Tirmaa-Klaar, 2011; Sliwinski, 2014a, 2014b), are primarily policy-oriented in nature and are accompanied by a contextually restricted understanding of power that is not necessarily easily applicable to other policies and contexts (Dunn, 2018). Addressing issues of power through empirical research, rather than conceptually, theoretically, or normatively, generally entails numerous challenges. These challenges are evident in the extensive literature written on various aspects of power in international relations and the efforts made to quantify it.

According to Dunn (2018), the EU assumes cyber power in various ways. Firstly, the EU recognizes the importance of cybersecurity and has developed policies and strategies to address cyber threats (Manners, 2002). The EU employs various instruments, institutions, and agencies to exercise different forms of cyber power, both internally and externally. Internally, the EU utilizes voluntary arrangements, incentives, dialogue, cooperation, and coordination to enhance its cyber power.

From an external perspective, the EU advocates a cooperation policy based on promoting cyberspace as an area of fundamental rights and freedoms. However, it is accepted that the EU lacks a unified strategic approach to intentionally wielding its cyber power. Although the EU has the capacity to utilize non-state cyber elements to support its policies, there is no clearly defined strategy to fully harness this power. As information technology becomes an increasingly central component in the convergence of security issues, it is recognized that any political actor with regional or global ambitions must engage in the cyber sphere. Therefore, it is suggested that the EU develop a kind of cyber power underpinned by resilience and the EU's core values, such as prevention, integrity, and multilateralism (Dunn, 2018). In short, the EU assumes cyber power through cybersecurity policies and strategies, using various instruments and agencies, both internally and externally. Nevertheless, the need to develop an integrated strategic approach to fully exercise its cyber power is acknowledged.

Conclusions

The transformation of cyberspace toward cyber power represents a fundamental change in the conception of power in the contemporary era. This change has been driven by technological advances that have turned cyberspace from a simple means of communication into a strategic field where battles are fought for influence, security, and supremacy. Cyber power not only implies the ability to control and manipulate cyberspace but also the ability to exert influence and achieve political, economic, and social objectives through digital means.

The diverse perspectives on cyber power reflect the complexity and multiple dimensions of this phenomenon. On one hand, some visions highlight the opportunities that cyberspace offers for innovation, collaboration, and citizen empowerment. From this perspective, cyber power is seen as a democratizing force that expands access to information, facilitates citizen participation, and stimulates economic and social development.

On the other hand, more critical approaches highlight the risks and challenges associated with cyber power. These visions caution against the growing vulnerability of critical infrastructure to cyberattacks, the erosion of privacy and security of personal data, and the potential for online manipulation and disinformation to undermine democracy and human rights.

In this context, understanding and addressing diverse perspectives on cyber power is crucial for designing effective policies and strategies that promote the responsible and ethical use of cyberspace. This involves strengthening cybersecurity, safeguarding individuals' digital rights, and fostering inclusive and transparent governance of cyberspace at both national and international levels. Ultimately, the challenge lies in harnessing the opportunities that cyber power provides to drive progress and human well-being while mitigating the risks and addressing the challenges posed by this new dimension of power in the 21st century.

References

- Alberts, D. S., & Hayes, R. E. (2003). *Power to the edge: Command... Control... in the information age*. CCRP Publication Series. http://www.dodccrp.org/files/Alberts_Power.pdf
- Arellano, A. (2019). *Ciberconflicto: La nueva amenaza global*. Instituto de Ingeniería UNAM.
- Barnett, M., & Duvall, R. (2005). Power in international politics. *International Organization*, 59(1), 39-75. <https://doi.org/10.1017/S0020818305050010>
- Bauman, Z. (2000). *Modernidad líquida*. Fondo de Cultura Económica.
- Cano, J. J. (2021). Los conflictos híbridos y el poder de los algoritmos. *Revista Sistemas*, (161), 62-72. <https://doi.org/10.29236/sistemas.n161a6>
- Carr, M., & Tikk, E. (2021). *International law and cyber conflict: Responding to new challenges*. Cambridge University Press.
- Castells, M. (1996). *La era de la información: Economía, sociedad y cultura* (Vol. 1, La sociedad red). Alianza Editorial.
- Castells, M. (2001). *La galaxia internet*. Plaza & Janes.
- Castells, M. (2010). *The information age: Economy, society, and culture* (Vol 1., The rise of the network society). John Wiley & Sons.
- Centro Superior de Estudios de la Defensa Nacional [CESEDEN]. (2012). *El ciberespacio: Nuevo escenario de confrontación*. Ministerio de Defensa Nacional. https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf
- Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. Harper Collins.
- Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: Un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, 18(30), 357-377. <https://doi.org/10.21830/19006586.588>
- DoD. (2011). *Department of Defense Dictionary of Military and Associated Terms*. DoD. https://irp.fas.org/doddir/dod/jp1_02.pdf
- Dunn, C. M. (2018). Europe's cyber-power. *European Politics and Society*, 19(3), 304-320. <https://doi.org/10.1080/23745118.2018.1430718>
- Estudillo, J. G. (2002). *Visibilidad de la producción académica de feministas mexicanas a través de una base de datos* [Bachelor's thesis, Universidad Nacional Autónoma de México].
- Ferreira da Silva, P. (2018). Oportunidades y desafíos de tecnologías emergentes: La importancia de la industria aeroespacial para Brasil. *Revista Fuerza Aérea-EUA*, (2), 36-48. https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%201%20Issue%202/Spanish/05-peterson_s.pdf

- Foucault, M. (1970). *El orden del discurso*. Fabula Tusquets Editores.
- Gibson, W. (1982). *Burning Chrome*. Ace Books.
- Gibson, W. (1984). *Neuromante*. Minotauro.
- Gómez Rodríguez, G. A. (2017). *Riesgos de transgresión moral del militar en la postmodernidad* [Thesis, Universitat de Barcelona]. Repositorio UB. https://diposit.ub.edu/dspace/bitstream/2445/119533/1/GAGR_TESIS.pdf
- Hardt, M., & Negri, A. (2004). *Multitud: guerra y democracia en la era del imperio*. Debate.
- Hunker, J. (2010). *Cyber war and cyber power: Issues for NATO doctrine* [Research Paper, N.º 62]. https://ciaotest.cc.columbia.edu/wps/nat/0031912/f_0031912_25908.pdf
- Jordan, T. (1999). *Cyberpower: The culture and politics of cyberspace and the internet*. Routledge.
- Kant, M. (1795/2010). *La paz perpetua*. Porrúa.
- Kern, S. (2015). *Expanding combat power through military cyber power theory* [Master's thesis, Joint Advanced Warfighting School]. Repositorio institucional. <https://apps.dtic.mil/sti/pdfs/ADA621664.pdf>
- Klimburg, A., & Tirmaa-Klaar, H. (2011). Cybersecurity and cyberpower: Concepts, conditions, and capabilities for cooperation for action within the EU. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET\(2011\)433828_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf)
- Kramer, F. D., Starr, S. H., & Went, L. K. (2009). *Cyberpower and national security*. Potomac Books, Inc.
- Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr & L. K. Wentz, *Cyberpower and National Security* (pp. 1-17). <https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/>
- Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
- Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *Isjlp*, (8), 321. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlp8&div=17&id=&page=>
- Libicki, M. C. (2018). Expectations of cyber deterrence. *Journal of Strategic Studies*, 41(1-2), 44-57. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-4/Libicki.pdf
- Lisa Institute. (n.d.) ¿Qué es la guerras híbridas y cómo nos afectan las amenazas híbridas. <https://www.lisainstitute.com/blogs/blog/guerra-hibrida-amenazas-hibridas#:~:text=En%20los%20C3%BAltimos%20a%C3%B1os%20cobran,o%20vectores%20de%20presi%C3%B3n%20econ%C3%B3mica>
- MacDonald, D. B. (2009). *Thinking history, fighting evil: Neoconservatives and the perils of historical analogy in American politics*. Lexington Books.

- Madden, D., Hoffmann, D., Johnson, M., Krawchuk, F., Nardulli, B. R., Peters, J. E., Robinson, L., & Doll, A. (2016, February 23). *Toward operational art in special warfare*. Rand Corporation. https://www.rand.org/pubs/research_reports/RR779.html
- Manners, I. (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies*, 40(2), 235-258. <https://doi.org/10.1111/1468-5965.003>
- Mitchell, W. J. (1995). *City of bits: Space, place, and the Infobahn*. MIT Press.
- Nye, J. S. (2010). *Cyber power*. Harvard Kennedy School.
- Nye, J. S. (2011). *The future of power*. Public Affairs.
- Pelroth, N. (2022). *Así es como me dicen que acabará el mundo*. Tendencias.
- Psychogiou, V. (2022) Cyberspace: Is NATO doing enough? <https://finabel.org/wp-content/uploads/2022/02/cyberspace-is-nato-doing-enough-1.pdf>
- Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5-32. <https://doi.org/10.1080/01402390.2011.608939>
- Sánchez, M. E. (2019). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. In G. Medina (Ed.), *La seguridad en el ciberespacio: un desafío para Colombia* (pp. 27-59). Escuela Superior de Guerra "General Rafael Reyes Prieto". <https://doi.org/10.25062/9789585216549.01>
- Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Crown.
- Schwab, K. (2017). *La cuarta revolución industrial*. Debate.
- Segal, H. (2017). *Cyber-security at a frantic time: A rational plan*. Canadian Global Affairs Institute.
- Singer, P. W., & Friedman, A. (2021). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- Sliwinski, K. F. (2014a). European union – Cyber power in the making. *Asia-Pacific Journal of EU Studies*, 12(1), 1-22. https://www.researchgate.net/publication/317717658_European_Union_-_cyber_power_in_the_making
- Sliwinski, K.F. (2014b). Moving beyond the European union's weakness as a cyber-security agent. *Contemporary Security Policy*, 35(3), 468-486. <https://10.1080/13523260.2014.959261>
- Stavridis, J., & Farkas, E. N. (2012). The 21st century force multiplier: Public–private collaboration. *The Washington Quarterly*, 35(2), 7-20. <https://doi.org/10.1080/0163660X.2012.665336>
- Tikk, E., & Kerttunen, M. (Eds.). (2020). *Routledge handbook of international cybersecurity*. Routledge.
- Toffler, A. (1970). *Future Shock*. Bantam House.
- Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.

- Valeriano, B., Jensen, B., & Maness, R. C. (2020). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.
- Vergara, E., Trama, G., Uriona, M. N., Ortiz, J. U., & Destro, L. A. (2018). *Operaciones militares cibernéticas: Planeamiento y ejecución*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. <https://cefadigital.edu.ar/bitstream/1847939/939/1/CAVIII%20-%20OMC%20DE%20VERGARA.pdf>



EDITORIAL **ESDEG**

Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace

This book provides an in-depth analysis of current trends, untangling the web of invisible yet potentially devastating threats and attacks brewing in networks. Disruptive technologies, rapidly replacing existing infrastructures, pose significant challenges for cybersecurity and national cyber defense. This leads to an important question: What is the impact of disruptive technologies and global logistics on ensuring security and defense in cyberspace?



ISBN 978-628-7818-05-7

