UNIVERSIDADE CATÓLICA PORTUGUESA

INSTITUTO DE ESTUDOS POLÍTICOS

Securing Cyberspace: Threats and Challenges to NATO

Mestrado em Ciência Política e Relações Internacionais: Segurança e Defesa

Ramo: Relações Internacionais

António Miguel Correia Semedo Neves Almeida - 100520012

Dissertação de Mestrado orientada por Professor Doutor Francisco Proença Garcia

Instituto de Estudos Políticos

Setembro 2023

Lisboa, Portugal

Aos meus pais,

pelo exemplo e força que sempre me deram.

Aos meus colegas,

pela amizade e espírito académico que muito me motivou ao longo desta etapa.

PAGE LEFT INTENTIONALLY BLANK

Acknowledgments

To begin, I would like to thank Universidade Católica Portuguesa, more specifically, the Instituto de Estudos Políticos, for being my home throughout my academic years and for the exceptional educational experiences and opportunities it has offered me throughout my academic journey. Additionally, I would like to express my appreciation to Professor Doutor João Carlos Espada, the Director of the Instituto de Estudos Políticos, for his unwavering commitment to upholding the high standards and noble objectives of this esteemed house.

I 'd also like to extend my appreciation to Prof.ª Doutora Ivone Moreira, the Coordinator of the Master's Degree program in Political Science and International Relations: Security and Defence. Her unwavering interest in my academic endeavours and her consistent support throughout my tenure in the program have been invaluable. I'm also grateful for her continuous guidance and advice during this period.

I am equally grateful to my thesis supervisor, Tenente-Coronel Francisco Proença Garcia, for his invaluable guidance and steadfast support during the process of crafting this thesis. His clear and succinct counsel played a pivotal role in shaping the content and direction of this research work. Without him, this thesis would not be what it is.

I would also like to express my gratitude to Dr.ª Susana Pedro for her unwavering patience and constant readiness to assist me whenever needed, consistently providing her expertise to the fullest extent.

I'd also like to extend my thanks to my friends and colleagues for their support and guidance during this period. Special mention goes to my friend Sofia Florentino, who consistently made time to review my work.

Finally, but certainly not least, I would like to express my heartfelt gratitude and love to my parents, to whom I dedicate this thesis.

PAGE LEFT INTENTIONALLY BLANK

Abstract

Cyberspace, and the topic of cyber, is today an issue of great importance. This thesis explores the significance of cyberspace and cyberspace security within the context of NATO and the current and future threats and challenges faced by the Alliance. In an interconnected world, cyberspace serves as a critical medium linking individuals, organizations, and vital infrastructures. However, it also presents an attractive target for malicious actors seeking to disrupt, steal information, or launch cyber-attacks. The emergence of hybrid warfare and information warfare further highlights the importance of securing cyberspace. The interconnectedness of critical infrastructure systems further emphasizes the need to protect cyberspace to ensure national security, economic stability, and public safety. As NATO operates on the principle of collective defence, strengthening cyberspace security enables the Alliance to respond collectively to cyber threats that transcend borders. Furthermore, as technology continues to advance, cyberspace security becomes even more crucial to address emerging risks and vulnerabilities. By prioritizing cyberspace security, NATO can enhance its resilience, promotes information sharing, and remain adaptable in the face of evolving cyber threats.

Keywords: *Cyberspace; Cyberspace security; Cybersecurity; Cyber defence; Cyber threats; Cyber-attacks; Disinformation; Misinformation; Critical infrastructure; Cyber-espionage; Europe; NATO.*

This thesis has approximately: **36,200** words

PAGE LEFT INTENTIONALLY BLANK

PAGE LEFT INTENTIONALLY BLANK

1. Introduction

Today, cyberspace has emerged as a subject of immense significance and relevance. It stands at the forefront of discussions and deliberations, commanding our attention like never before. This thesis embarks on a comprehensive exploration of the multifaceted importance of cyberspace and, by extension, the paramount issue of cyberspace security, particularly within the context of the North Atlantic Treaty Organization (NATO). This will be done by posing and exploring a key research question: "**what threats pose a challenge to NATO's abilities to secure cyberspace and how can these difficulties influence NATO and its member-states?**" To help answer this question, three sub-questions will need to be explored throughout this thesis; these are essential to our comprehension of cyberspace and cyberspace security.

With the world interconnected in a global landscape, cyberspace serves as a vital conduit, seamlessly linking individuals, organizations, governments, and critical infrastructures. Its significance transcends boundaries and sectors, becoming an indispensable element of our modern society and existence. The very fabric of our daily lives, from communication and commerce to healthcare and governance, is intricately woven into the digital tapestry of cyberspace. This is where we will begin, by posing the question: "How has Cyberspace Security evolved within NATO?"

The contemporary security landscape has witnessed the emergence of hybrid warfare and information warfare, where the boundaries between physical and digital conflicts blur. In this new paradigm, the manipulation of information and the covert use of cyber capabilities play pivotal roles. These developments underscore the criticality of securing cyberspace, not only as a technical challenge but as a fundamental aspect of national and international security. NATO, and each of its member-states, have their own different methods of approaching these

modern challenges; but what are these different approaches? This second question we will explore further in the third and fourth chapters.

In this vast and interconnected domain, vulnerabilities and threats abound. Malicious actors, ranging from state-sponsored entities to cybercriminals, continually probe and exploit weaknesses in cyberspace's defences. Their objectives span a spectrum from disruption and theft of sensitive information to launching sophisticated cyberattacks that can have far-reaching consequences. Furthermore, the interdependence of critical infrastructure systems elevates the importance of safeguarding cyberspace. The reliable functioning of essential services, including energy, transportation, healthcare, and finance, relies heavily on secure digital networks. Any disruption in cyberspace can reverberate throughout society, potentially jeopardizing national security, economic stability, and public safety. Here we must ask our third and final question: “what are the most concerning threats facing NATO, and what effects can they have on the Alliance?”

This thesis delves deep into the multifaceted dimensions of this critical domain within the framework of NATO. By doing so, it seeks to shed light on the current and future threats and challenges faced by the Alliance in safeguarding the digital realm.

1.1. Methodology

This thesis comprises six chapters. The initial chapter provides a concise introduction to the concepts of cyberspace and cyberspace security, highlighting the threats present in this domain that could potentially be employed against the Alliance. In the second chapter, we delve into the historical evolution of cyberspace security within NATO, constructing a timeline that illustrates the Alliance's gradual shift toward a heightened emphasis on cyber and cybersecurity. This chapter seeks to address the first sub-question posed. Moving forward, the third chapter will delve into NATO's strategy regarding cyberspace security, examining its

institutional framework and agencies, as well as its collaborative cyber partnerships. The subsequent fourth chapter will similarly investigate the diverse approaches adopted by specific member states in addressing their respective cyberspace security challenges, elucidating the spectrum of offensive and defensive strategies employed. Both the third and fourth chapters are aimed at addressing the second sub-question presented. In the fifth chapter, we will identify and investigate the cyber threats that are of greatest concern and pose significant challenges to NATO and its member states, particularly those that may prove difficult to mitigate or prevent. This chapter is dedicated to addressing the third and final sub-question posed within this thesis.

This thesis is written in the English language (United Kingdom) and follows the Chicago style of referencing. The primary sources of research and investigation within this thesis consist of four interviews; three conducted on-site, and one conducted remotely by telephone. The interviewees were as follows: Brigadier General Paulo Viegas Nunes, NCI Academy's first (acting) Director; Rear-Admiral António Gameiro Marques, the Director of the Portuguese National Office of Security (*Gabinete Nacional de Segurança*); Engineer Lino Santos, Coordinator of the Portuguese National Cybersecurity Centre; and Manuel Poêjo Torres, a specialist on NATO and international relations. The interviews were conducted in the Portuguese language. The translated (English) interview transcripts, as well as the original (Portuguese) interview transcripts, can both be found in the Appendix chapter of this thesis, and citations within the thesis refer to the corresponding section and page number(s) in the Appendix chapter.

The secondary sources of research are mainly of a qualitative nature but include certain elements of a quantitative nature. These include official reports published by NATO and the CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence), national cybersecurity and cyber defence strategies, information available publicly on relevant official websites, institutional projects, journal articles, scholarly publications, and news articles when necessary.

This thesis also includes graphs and other illustrative models sourced from official documents, scholarly publications, and institutional projects. These figures are strategically placed throughout the thesis, within their pertinent contexts, instead of being relegated to the Appendix chapter. Likewise, quotations were also placed throughout the thesis within the text.

1.2. State of the Art

Cyberspace Security has become an indispensable element to national security, with disturbances within the realm of cyberspace having the potential to echo across society, posing risks to national security, economic stability, and public safety. This has, naturally, attracted NATO's attention and that of its member-states. As we shall see further ahead in the following chapters, in 2016 the Alliance formally recognized cyberspace as a domain of conflict[1] and has since then implemented a series of policies, established agencies and other operational centres with the clear objective of seamlessly integrating the cyber domain into both military operations and the development of allied capabilities.

However, there remains a diversity of approaches to cyber defence within NATO's major member countries. These approaches can be broadly categorized into those nations pursuing a more proactive and offensive stance in cyberspace security, and those that opt for a more defensive posture. The reasons behind this vary and will be explored further in the chapters ahead. Nonetheless, the rapidly evolving nature of cyberspace and its threats continues to challenge the Alliance in developing a unified and cohesive approach within its framework that effectively safeguards the security, stability, and resilience of its member-states.

[1] "Warsaw Summit Communiqué," *NATO*, July 9, 2016, NATO, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Reports and papers, such as those written by Susan Davis and published by the NATO Parliamentary Assembly's Science and Technology Committee[2], and Manuel Poêjo Torres[3], respectively, offer a clear and concise outline of the realities and threats facing NATO's cyberspace security, as well as its capabilities. Manuel Poêjo Torres' paper describes the many emerging threats facing NATO, and how the Alliance faces increasing challenges in adapting to said threats. It also uses the "Red Queen Hypothesis" and the "Court Jester Hypothesis" to analyse the trends and evolution of cyberspace. These two evolutionary theories are applied to the evolution of cyberspace. The "Red Queen Hypothesis" suggests that the evolution of cyberspace and its actors is driven by biotic factors, such as the competitive proliferation of cyber capabilities between opposing powers. Conversely, the "Court Jester Hypothesis" contends that the primary driving force behind the evolution of cyberspace and its actors is abiotic factors, such as external and uncontrollable changes, rather than biotic factors. Another aspect of this paper is delving into how cyberspace fits into modern conflicts and operations, and how said conflicts and operations have become hybrid – or "cybrid" as he puts it – as well as its role and importance to a nation's sovereignty.[4]

Articles such as those written by André W.M. Gerrits[5], Jeffrey B. Jones[6], Rui Piteira Natário and Paulo Viegas Nunes[7], Hannah Marshall and Alena Drieschova[8] allow us to

[2] Susan Davis, *NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE* (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019).
[3] Manuel Poêjo Torres, William Hasselberger, and Francisco Proença Garcia, "The Atlantic Posture and the 'Cybrid' Threats of Tomorrow," essay, in *O PODER AUTORITÁRIO E O DESAFIO PARA AS DEMOCRACIAS LIBERAIS* (Óbidos, Portugal: Alêtheia Editores, 2022), 130–69.
[4] Ibid.
[5] André W.M. Gerrits, "Disinformation in International Relations: How Important Is It?," *Security and Human Rights* 29, no. 1–4 (2018): 3–23, https://doi.org/10.1163/18750230-02901007.
[6] Jeffrey B. Jones, "Confronting China's Efforts to Steal Defense Information," Harvard Kennedy School Belfer Center for Science and International Affairs, May 2020, https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.
[7] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014), https://www.revistamilitar.pt/artigo/913.
[8] Hannah Marshall and Alena Drieschova, "Post-Truth Politics in the UK's Brexit Referendum," *New Perspectives* 26, no. 3 (2018): 89–105, https://doi.org/10.1177/2336825x1802600305.

understand the most prominent threats facing the Alliance today. André W.M. Gerrits' article explores disinformation in international relations, including strategies to combat it, and how international organizations, such as NATO, the European Union, and the Organization for Security and Co-operation in Europe (OSCE), could foster confidence-building initiatives. It emphasizes that disinformation's security impact shouldn't be overstated, and like in domestic politics, it exploits existing divides and concerns, disrupting the international landscape.[9] Similarly, Hannah Marshall and Alena Drieschova's paper examines the role of post-truth politics in the Brexit referendum, asserting that Brexit serves as a prime example of post-truth politics in the United Kingdom. More importantly, it identifies two main factors: the impact of social media and online news consumption – which allows for unchecked dissemination of (dis)information – and a growing distrust in established institutions, political elites, experts, and traditional media.[10] In Jeffrey B. Jones' piece, he thoroughly examines the expanding scale and frequency of China's cyber espionage activities, highlighting the growing challenge they pose. The article also delves into the potential risks these practices pose to national security and defence and offers insights into potential strategies to more effectively counter this cyber threat.[11] Rui Piteira Natário and Paulo Viegas Nunes article looks at another concern we will explore in this thesis: that of critical infrastructure. It explores the increasing interdependence of these critical infrastructures, as well as the vulnerabilities facing these systems and their impact should they fall victim to a relatively potent and sophisticated cyber-attack.[12]

[9] André W.M. Gerrits, "Disinformation in International Relations: How Important Is It?," *Security and Human Rights* 29, no. 1–4 (2018): 3–23, https://doi.org/10.1163/18750230-02901007.
[10] Hannah Marshall and Alena Drieschova, "Post-Truth Politics in the UK's Brexit Referendum," *New Perspectives* 26, no. 3 (2018): 89–105, https://doi.org/10.1177/2336825x1802600305.
[11] Jeffrey B. Jones, "Confronting China's Efforts to Steal Defense Information," Harvard Kennedy School Belfer Center for Science and International Affairs, May 2020, https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.
[12] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014), https://www.revistamilitar.pt/artigo/913.

Likewise, articles and reports such as those written by Sungbaek Cho[13], Mauno Pihelgas[14], Florian Skopik and Timea Pahi[15] provide solutions and methods to effectively attribute, counter and/or prevent these ever-sophisticated cyber threats. Sungbaek Cho's paper offers an examination of the security attributes specific to industrial control systems used in critical infrastructure, emphasizing significant cyber threats, vital security precautions, and methods for conducting cybersecurity risk management, as well as exploring national government's responsibilities in safeguarding critical infrastructures and elevating cybersecurity measures.[16] Mauno Pihelgas' report addresses the challenges associated with establishing accurate attribution in the aftermath of cyber-attacks. It specifically focuses on cases where the responsible entity behind the attack is either unknown (no-flag) or deliberately obscured (false-flag) for various reasons.[17] Florian Skopik and Timea Pahi's article underscores the often-neglected issue of attributing cyber-attacks. It explains how secret services are particularly invested in determining whether an attack was executed on behalf of a nation state. It likewise examines the various methods and tools in network and computer forensics used to gather evidence to form the foundation for linking cyber actions to cyber actors. the paper highlights a less-explored issue: false flag campaigns, which use covert tactics to mislead attribution efforts and also provides an overview of attack techniques, discusses the

[13] Sungbaek Cho, "Enhancing Cybersecurity of Industrial Control Systems," essay, in *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)*, ed. USAWC Press (Carlisle, PA: Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022), 355–85.
[14] Mauno Pihelgas, ed., "Mitigating Risks Arising from False-Flag and No-Flag Cyber Attacks," CCDCOE, March 31, 2015, https://ccdcoe.org/uploads/2018/10/False-flag-and-no-flag-20052015.pdf.
[15] Florian Skopik and Timea Pahi, "Under False Flag: Using Technical Artifacts for Cyber Attack Attribution," *SpringerOpen* 3, no. 8 (March 20, 2020), https://doi.org/https://doi.org/10.1186/s42400-020-00048-4.
[16] Sungbaek Cho, "Enhancing Cybersecurity of Industrial Control Systems," essay, in *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)*, ed. USAWC Press (Carlisle, PA: Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022), 355–85.
[17] Mauno Pihelgas, ed., "Mitigating Risks Arising from False-Flag and No-Flag Cyber Attacks," CCDCOE, March 31, 2015, https://ccdcoe.org/uploads/2018/10/False-flag-and-no-flag-20052015.pdf.

traces they leave, and their relevance in identifying false flag campaigns, while also evaluating the ease with which traces can be manipulated.[18]

Reports and papers such as those written by Piret Pernik, Jesse Wojtkowiak and Alexander Verschoor-Kirss (published by the NATO Cooperative Cyber Defence Centre of Excellence)[19], Marios Panagiotis Efthymiopoulos[20], Alessandro Marrone and Ester Sabatino[21], explains the different methods and approaches taken by certain and relevant NATO member-states, as well as NATO as a whole. Marios Panagiotis Efthymiopoulos' article emphasizes the significance of cybersecurity as a policy concern and underscores the need for continuous improvement in NATO's cyber strategy, management, and operations, and proposes a strategic realignment framework that prioritizes practical innovation and entrepreneurship, operational efficiency, and strengthened political cooperation for field operations. The article explicitly evaluates NATO's security and cyber-security options for the near future and introduces a new collective defence format.[22] Lastly, Alessandro Marrone and Ester Sabatino's paper offers a succinct and lucid portrayal of the multitude of priorities and goals confronting some leading NATO member-states – such as the United States, the United Kingdom and Germany – and aids in creating a comprehensive understanding of the current state of cyberspace security within NATO itself.[23]

---

[18] Florian Skopik and Timea Pahi, "Under False Flag: Using Technical Artifacts for Cyber Attack Attribution," *SpringerOpen* 3, no. 8 (March 20, 2020), https://doi.org/https://doi.org/10.1186/s42400-020-00048-4.
[19] Piret Pernik, Jesse Wojtkowiak, and Alexander Verschoor-Kirss , "National Cyber Security Organisation: UNITED STATES," CCDCOE, 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf.
[20] Marios Panagiotis Efthymiopoulos, "A Cyber-Security Framework for Development, Defense and Innovation at NATO," *Journal of Innovation and Entrepreneurship* 8, no. 1 (2019), https://doi.org/10.1186/s13731-019-0105-z.
[21] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models.
[22] Marios Panagiotis Efthymiopoulos, "A Cyber-Security Framework for Development, Defense and Innovation at NATO," *Journal of Innovation and Entrepreneurship* 8, no. 1 (2019), https://doi.org/10.1186/s13731-019-0105-z.
[23] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models.

1.3. Understanding the Concepts of Cyberspace, Cyberspace Security, and Cyber Threats

To understand "Cyberspace" and "Cyberspace Security" we must first understand how the "Internet" functions. The Internet, often referred to as a global network of networks, is a complex infrastructure that enables seamless communication and information exchange across the globe. It functions through the use of various interconnected devices, including computers, servers, and routers, all working together to transmit data and facilitate connectivity. At the heart of Internet communication are protocols, which are universally accepted rules that dictate how data is transmitted and received. These protocols ensure that messages are correctly formatted, transmitted, and interpreted by devices on the network. They establish the standards for data exchange, such as the Internet Protocol (IP), which assigns unique addresses to each device connected to the Internet. When a user wants to access a website, they enter the website's name, known as a domain, into a web browser's address bar. This request is then sent to a Domain Name Server (DNS), which acts as a lookup service. The DNS translates the domain name into the corresponding IP address associated with the website. This conversion allows the user's computer to locate and establish a connection with the server hosting the requested website. To reach the intended destination, the request travels through a series of routers. Routers are devices that determine the most efficient path for data packets to follow based on network conditions and routing tables. Each router examines the packet's destination address and forwards it to the next hop along the path until it reaches the desired IP address.[24]

Internet communication relies on a concept called packet switching. Instead of transmitting data as one continuous stream, it is divided into smaller units called packets. Each

[24] Jeffrey B. Jones, "Confronting China's Efforts to Steal Defense Information," Harvard Kennedy School Belfer Center for Science and International Affairs, May 2020, https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.

packet contains a portion of the data, along with the necessary addressing information. These packets are individually routed through the network, often taking different paths to reach the destination. Once all the packets arrive at the recipient's computer, an Internet protocol reassembles them in the correct order, allowing the intended information to be displayed or utilized. This packet-switching approach offers several advantages, including increased efficiency, robustness, and the ability to handle various types of data traffic simultaneously. It also enables seamless communication even if certain network components experience congestion or disruption, as packets can be rerouted dynamically to alternative paths. Overall, the functioning of the Internet and its communication processes involve a sophisticated combination of protocols, routing mechanisms, and data handling techniques. Together, they ensure reliable and efficient transmission of information across the vast interconnected network, making the Internet an invaluable tool for global connectivity and information exchange.[25]

Now we shall move onto “Cybersecurity” or “Cyberspace Security” and how to define it. There are many possible definitions of what cybersecurity is, not all in accordance with each other, as Eng. Lino Santos puts it.[26] Some may see cybersecurity as a subset of information security, a much wider and general view of information technology (IT) security, rather than a distinctive and separate type of security, while some see it as an emerging type of security that has developed, and is now emancipating itself, from the wider information security, not unlike how the United States Space Force, which was once a part of the United States Air Force, has now become an independent and separate military service branch, with its own commandant. Others have also considered that information security and cybersecurity are distinct from each other, where the scope, motives, as well as method of an attack are determinant to whether it

[25] Ibid.
[26] António Miguel Neves Almeida and Lino Santos, Interview: Coordinator Lino Santos, personal, February 13, 2023. Refer to Appendix III, p. 196.

belongs within the cybersecurity category or the information security, the latter being considered lower-level type security. Other definitions state that "*cyber security focuses more on integrity and availability whereas information security is mainly concerned with confidentiality*."[27] Some governmental sources on the other hand do not concretely give a specific or straightforward definition on what cybersecurity is, with some stating that there is no universally accepted definition of what cybersecurity is. The NATO Parliamentary Assembly's Science and Technology Committee's 2019 report goes deeper, dividing cybersecurity and cyber-defence, and making use of the U.S. Department of Defence's "Dictionary of Military and Associated Terms" to define both terms. The report shortens the DOD Dictionary's definition slightly, but essentially defines cybersecurity, or "cyberspace security", as "*[a]ctions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation*"[28], and defines cyber-defence, or "cyberspace defence", as "*[a]ctions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration.*"[29] Essentially they divide cybersecurity as an act of preventing a breach in the system, while cyber-defence as an act of repelling an attack in an already breached system. The definitions vary depending on the source, be it

[27] Daniel Schatz, Rabih Bashroush, and Julie Wall, "Towards a More Representative Definition of Cyber Security," *The Journal of Digital Forensics, Security and Law* 12, no. 2 (June 30, 2017): 55–57, https://doi.org/10.15394/jdfsl.2017.1476, 56.
[28] U.S. Department of Defence, ed., "Cyberspace Defence," in *Department of Defense Dictionary of Military and Associated Terms (Incorporating the NATO and IADB Dictionaries)* (Washington, D.C., United States of America: Joint Chiefs of Staff, 1987), 55.
[29] Ibid.

governmental/state definitions, or academic definitions, and can be highly subjective and in some cases even uninformative. This ambiguity and lack of a straightforward definition can lead to challenges when it comes to agreements regarding cyber arms control, especially when definitions and even terminology vary greatly from major power to major power, these being the United States of America, China, and Russia, making it more difficult to find a common ground when discussing potential agreements.[30]

We can however define cybersecurity as the practice of defending and protecting software and data as well as it's hardware; the same way software can be protected via firewalls for example, hardware can be physically protected as well, for example a server being locked in room to keep it from being physically accessed. With this starting definition we can begin to branch off into the types of security within cybersecurity. These types of security include, but are not limited to, network security, application security, information security, and operational security. Network security, as we shall see, is very important within NATO, and it involves protecting a network from any cyber-attack, including keeping any dangerous malware out of a network. Application security essentially means ensuring threats are kept out of software and respective devices, something that is accomplished in the development stages of said software, long before it is ever released for use. The inability to guarantee that fundamental security could lead to intruders gaining access to users' information; the effort will need to be doubly so if the software in question is designed to serve as security, i.e., an antivirus software. Information security means the ability to protect information and data, be this information stored away in a server or be it in "transit", keeping it from being intercepted or copied from point A to point B. Operational security focuses more on managing permissions, such as who has access to what, or where and how data may be stored or with who the said

[30] Daniel Schatz, Rabih Bashroush, and Julie Wall, "Towards a More Representative Definition of Cyber Security," *The Journal of Digital Forensics, Security and Law* 12, no. 2 (June 30, 2017): 55–57, https://doi.org/10.15394/jdfsl.2017.1476.

data can be shared with. Guaranteeing operational success is imperative when discussing a military alliance such as NATO. We will see further on why within NATO such operational security is invaluable, considering the sensitive and potentially classified information NATO deals with. Operational security could, in not so extreme cases, mean not only operational success, but also guaranteeing NATO's upper hand against its rivals.[31]

Security can also come in the form of guidelines that advise people on how to behave online and offline with regards to computers. Many times, despite the added layers of security and checks and double-checks, and due to a simple lack of knowledge and knowhow, people/employees may ultimately become a variable that cause a breach, by accidently introducing a virus that opens a backdoor to intruders, either via an unidentified pen drive, or opening a suspicious email. This is where the aforementioned guidelines come in; it is extremely important to educate those that may have access to an organization's system and network. As mentioned before, opening suspicious emails and its attachments or plugging in an unknown pen drive may lead to a breach; educating people to refrain from such conducts and on how to behave when confronted with these situations is another aspect of cybersecurity and a step to guaranteeing a securer system. However, when security fails, contingency plans must be implemented to respond to a security breach and to safeguard system functionality and the information therein; this is where operational continuity and disaster recovery comes in. In the event of a cyber-attack or a security breach in the system, organizations tend to fall back to what is known as operational continuity, which essentially means trying to operate without a certain system; the degree of systems available will depend on the scope of the intrusion and the systems that may have been affected by it. It can be compared to sailing and, attempting to repair, a ship through a storm, where difficulty may vary and the ship itself is crippled. Disaster

[31] Kaspersky, "What Is Cyber Security?," www.kaspersky.com, May 16, 2022, https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

recovery, as the name would suggest, is the protocol an organization activates to guide it and the affected system back to its original operating capacity before the security breach. It is the process to restore operations as well as information that may have been affected.[32]

We have seen what cybersecurity is, now we shall take a look at the general potential threats that may be encountered in cyberspace. These can be divided into three types of threats, each different from the other and each can have larger or smaller consequences; these are "cybercrime", "cyber-attacks", and "cyberterrorism". The first, cybercrime, is the practice of targeting systems for financial gain, usually in the form of ransomware – which we will see ahead – to hold a system "hostage" in exchange for a monetary ransom. This type of threat can be perpetrated by one or more actors; although usually carried out by unaffiliated criminals, they may in some cases be state sponsored or have political motivations behind it. The second, cyber-attacks, are the more well-known and are sometimes used as a general term for cyber threats; more often than not these attacks involve a group of actors rather than a singular actor, and the purpose behind these attacks is the gathering and acquisition of varying types of information within a system. These attacks are usually politically motivated and/or may be state sponsored and are associated to cyber-espionage. Finally, we have cyberterrorism, which are usually carried out by states as most of the time only states have the capabilities and resources to conduct such operations. The objective of cyberterrorism is a widespread attack to cripple a country's systems and infrastructure and in turn cause degree of fear and panic on the country's population. From these three types of threats, we can begin to explore how exactly these are carried out, in a practical sense. The first and more well-known type is "malware", which is a diminutive for "malicious software"; since malware comes subdivided into different types, malware can be used for a myriad of different reasons (such a criminal or political) and can be introduced into the systems through different ways, such as emails or by downloading

[32] Ibid.

a seemingly innocent looking file. A brief overview of how – according to the NATO Parliamentary Assembly's Science and Technology Committee (STC) – cyber operations succeed in gaining access to a system or network via the use of malicious software is essential to further our understanding further. Cyber operations tend to employ the use of malicious computer code to gain access to a system or network. To succeed, the intruder conducting said operation must find a vulnerability within the system and exploit it, either via a defect or a bug in the targeted system; they must then gain access to the targeted system, which can be done through remote access, covert operations, through the "supply chain" or by "*witting or unwitting insiders*"[33]; there they must deliver the malware payload to carry out the intended action.[34] Now, malware can be subdivided into "viruses", "trojans", "spyware", "ransomware", "adware", and "botnets". Viruses, like the real-world counterpart, replicates itself once inside the system and attempts to corrupt files with malicious code, rendering them useless and inoperable, and in some case unrecoverable. Trojans take their name from the Trojan Horse used by the Greeks to sneak into the city of Troy; following the same logic, a trojan disguises itself as legitimate and innocent software, deceiving the user into downloading it onto the system, once inside, the trojan spreads within the system and can either damage files or collect data within a system, or both. Spyware is similar to trojans, but unlike trojans remain undetected, and are used to, as the name would suggest, spy on a user or the system it's been inserted into. Once introduced, and unbeknownst to the user, the spyware will begin to discreetly gather information and spy on the user to gain relevant information, such as credit card information or passwords used to access different website; spyware can remain undetected in a system for a considerable amount of time. Criminals make use of this type of malware, but it can also be used my states to spy on another country's systems, gathering their secrets or

[33] Susan Davis, *NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE* (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 3.
[34] Ibid.

gaining access to their trademarked content;[35] a good example of this is China's abundant use of spyware to get ahead in their industrialization to surpass western countries such as the United States, with many Chinese "advancements" being stolen from American companies, as we shall see further ahead.[36] Ransomware, as mentioned above, is used to lockdown or restrict parts of a system, essentially taking it hostage, in return for a ransom; these have been used by criminals on banks, hospitals, and other businesses and organizations that depend greatly on their information systems, since the greater one depends on an IT system, the more likely they will be to pay the ransom instead of trying to regain access to their system their own way, which will take longer. With the increase of ransomware attack over the years, companies have begun to invest greatly in their own cybersecurity, incentivised by governments, as this may have greater consequences beyond a simple business, and may in fact potentially cripple a state's services and infrastructure, as we will explore further ahead. Adware is essentially a way to spread malware through online advertisements designed to incentivise a user into clicking on it, such as pop-up windows congratulating one for winning a prize. Finally, botnets are networks of hijacked computers that a criminal can use to perform tasks online without a user knowing about it, much like using a stolen vehicle to rob a bank.[37] Aside from malware we have other ways intruders can choose to break into a system or to achieve their objectives; one of these other ways is called "phishing", similar to the word "fishing" the concept is the same: deceiving a victim into giving them what they want through a bait that looks like something different from what it really is. This is usually used to trick a user, usually through an email, into giving them information the intruders want, such as credit card information; they do this

[35] Clare Stouffer, "10 Types of Malware + How to Prevent Malware from the Start," Norton, August 27, 2021, https://us.norton.com/blog/malware/types-of-malware.
[36] Jeffrey B. Jones, "Confronting China's Efforts to Steal Defense Information," Harvard Kennedy School Belfer Center for Science and International Affairs, May 2020, https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.
[37] Clare Stouffer, "10 Types of Malware + How to Prevent Malware from the Start," Norton, August 27, 2021, https://us.norton.com/blog/malware/types-of-malware.

by sending users an email, or a SMS message in some cases, pretending to be an official bank message, and if the message looks legitimate the users have no reason to distrust it and send their information willingly. For this reason, many businesses that deal with sensitive information usually send clients informative emails and messages stating that they will never ask for personal information, warning clients to avoid sending their information in any circumstance. Since this can also apply to businesses and organizations, many focus on staff training, as mentioned above, to avoid a breach in their systems due to a careless worker. Through the art of deception and disguise someone is able to pull in a "fish", so to speak. Another type of attack can come through what is known as "man-in-the-middle"; this is done when a man in the middle, i.e., the criminal, intercepts communications and information on an unsecured network. This usually happens on unsecured networks, such as a public Wi-Fi network accessible to all with no password protection, this is why it is advised to avoid accessing or inputting personal or sensitive information on public networks or avoid connecting to them altogether.[38] Finally, we have "denial-of-service" (DOS), and "distributed denial-of-service" (DDOS) attacks, which essentially means denying functionality to a system; a system is flooded with traffic to a point where it is incapable of functioning properly or at all. Unlike cyber operations conducted through the use of malware, DOS attacks do not require a flaw and does not exploit vulnerabilities in a system, rather it floods and overwhelms with an abundance of network traffic, making the system, the quantities introduced within, unmanageable.[39] A good example of this is when a ticket booth website gets flooded with clients wanting to purchase tickets for a popular concert; if the system is incapable of handling large amounts of

[38] Kaspersky, "What Is Cyber Security?," www.kaspersky.com, May 16, 2022, https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.
[39] Susan Davis, *NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE* (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 3.

traffic it will crash, DOS attacks simulate this, rendering a system inoperable or with extremely slow response times.[40]

[40] Kaspersky, "What Is Cyber Security?," www.kaspersky.com, May 16, 2022, https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

2. Evolution of Cyberspace Security within NATO

We have seen what cyberspace security is and what it entails, now we must look at how it has evolved throughout the years with NATO. As we know, there are three "traditional" domains of conflict: land, sea, and air, and it has been so since air vehicles were weaponized to be used in war; before that there was only land and sea. Since the weaponization of air vehicles, a new domain emerged, and within that domain new ways of defence emerged as well, and so the whole reality of war changed with it and adapted to the new circumstances. In this new age two new domains of conflict have emerged: space and cyberspace, resulting in the existence of five domains of conflict. Space has been, throughout the years the subject of many armed forces' evolution, with the creation of new branches within the armed forces, much like how the air force became a branch of its own. Many countries began to implement a space command within their air force and have gradually emancipated that space command into its own branch of the armed forces with its own command structure; the most recent and well-known case is the creation of the U.S. Space Force in 2019, once part of the U.S. Air Force, is now its own branch. This is not the only case however, in fact, the creation of the U.S. Space Force comes quite late compared to their Russian and Chinese counterparts, the Russian Space Forces (founded in 2015) and the People's Liberation Army Strategic Support Force (founded in 2015), respectively. We see the same happening here with this even newer domain of conflict, the same processes, the same gradual recognition and progressive adaptation regarding security and defence within this new domain, for example how the People's Liberation Army Strategic Support Force not only applies to space but also to cyberspace. It is through this gradual and progressive evolution that NATO and the West can defend against the rising tide of cyber threats, much like how anti-air guns or newer more effective planes were developed to counteract the then new threats that came from the sky. Cyberspace and cyberspace security is no different in that regard.

We will go back to 2002, where the NATO Summit was held in Prague; this was the summit that NATO agreed to place cybersecurity and defence on the Alliance's political agenda.[41] While NATO had always protected their information systems and their communications, it became apparent that cyberspace was not only beginning to play a role as a domain of conflict, but that it would indeed play a much larger role going forward, and so therefore it was vital to take cyberspace and its defences more seriously. In 2006, the NATO Summit in Riga declared the continued need to reinforce cybersecurity capabilities, so that NATO Allies can share information, data and intelligence in quicker and more reliable way, as well as guaranteeing greater protection.[42] In 2007 an unprecedented cyber campaign against Estonia left its public and private institutions crippled from multiple cyber-attacks, mostly DOS attacks. These cyber-attacks carried out by Russia were in response to Estonia's decision to remove a Soviet-era statue called the "Bronze Soldier of Tallinn" from a cemetery where many Soviet soldiers were buried. The never-before-seen nature of these attacks, be it methods, be it scope, led NATO to create in 2008 the "NATO Cooperative Cyber Defence Centre of Excellence", or "CCDCOE", and to the development of the "Tallinn Manual on the International Law Applicable to Cyber Warfare" by the latter, being published in 2013 and the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" published in 2017.[43] The aim of the Tallinn Manuals is to outline existing international laws applicable in cyberspace and has helped in the establishment of an international norm of conduct within cyberspace. It is important to note that the CCDCOE, while a NATO centre of excellence, is not, in fact, linked to the NATO Command Structure. In August of 2008, the Russo-Georgian War began, where Russia conducted many DOS cyber-attacks against Georgian news agencies

[41] "Prague Summit 2002 - Selected Documents and Statements," *NATO*, 2002, NATO, https://www.nato.int/docu/0211prague/speeches-e.pdf, 50-3.
[42] "Riga Summit Declaration," *NATO*, November 29, 2006, NATO, https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en.
[43] László Kovács, "CYBER SECURITY POLICY AND STRATEGY IN THE EUROPEAN UNION AND NATO," *REVISTA ACADEMIEI FORŢELOR TERESTRE* 1, no. 89 (2018): 16–24.

and government websites, such as the Georgian President's website. This became an example of how cyberwarfare could be used with conventional warfare for disastrous yet effective results; it showed the potential of that these cyber-attacks could have.[44]

With that revelation, NATO approved and adopted a new Strategic Concept at the 2010 NATO Summit held in Lisbon; in this Strategic Concept, NATO recognizes the scope to which cyber-attacks can reach as well as the accessibility of such methods, stating that "*[Cyber-attacks] are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks.*"[45] What came out of the 2010 Lisbon Summit was the second NATO Policy on Cyber Defence, approved in 2011, which set out the following points: Integration of cyber defence considerations into NATO structures and planning processes in order to perform NATO's core tasks of collective defence and crisis management; focus on prevention, resilience and defence of critical cyber assets to NATO and Allies; development of robust cyber defence capabilities and centralising protection of NATO's own networks; development of minimum requirements for cyber defence of national networks critical to NATO's core tasks; provision of assistance to the Allies to achieve a minimum level of cyber defence and reduce vulnerabilities of national critical infrastructures; and engagement with partners, international organisations, the private sector and academia.[46] It was also decided in this Summit that NATO's fourteen (14) agencies would be reformed into three streamline

[44] NATO, "Cyber Defence," NATO, July 14, 2022, https://www.nato.int/cps/en/natohq/topics_78170.htm.
[45] NATO, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization § (2010), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, 11.
[46] NATO, *Defending the Networks - The NATO Policy on Cyber Defence* (NATO Graphics & Printing, 2011).

programmatic categories, these being "procurement", "support", and "communications and information",[47] the latter being a major focus of this thesis, as we shall see ahead. In the following year cyber defence was introduced into NATO's Defence Planning Process (NDPP); the NDPP's aim is to "*provide a framework within which national and Alliance defence planning activities can be harmonised to enable Allies to provide the required forces and capabilities in the most effective way.*"[48] During NATO's 2012 Summit in Chicago, the Allies decided to improve the Alliance's cyber defences and its cyber defence capabilities even more, and decided to centralise all of NATO's networks, considering it is more effective and simpler having all these networks centrally protected rather than individually protected. In the same year, when NATO's agencies underwent reforms established at the 2010 Lisbon Summit, the NATO Communications and Information Agency (NCIA) was created, currently headquartered in Brussels, Belgium. The NCIA is a merger of five NATO agencies – the NATO C3 Organisation, NATO Communication and Information Systems Services Agency (NCSA), NATO Consultation, Command and Control Agency (NC3A), NATO Air Command and Control System Management Agency (NACMA), and NATO Headquarters Information and Communication Technology Service (ICTM).[49] The increasing importance of cyberspace and cyber defence leads to decisions being taken and implemented in a matter of months rather than years.[50]

As we had seen 2012 was a year of great change for reforming institutions and agencies dealing with cyber defence; 2014 would also be a year for change in that regard. In that year the North Atlantic Council (NAC) agreed on the renaming of the Defence Policy and Planning

[47] "Lisbon Summit Declaration," *NATO*, November 20, 2010, NATO, https://www.nato.int/cps/en/natolive/official_texts_68828.htm.
[48] NATO, "NATO Defence Planning Process," NATO, July 9, 2021, https://www.nato.int/cps/en/natohq/topics_49202.htm.
[49] NATO, "NATO Communications and Information Agency (NCI Agency)," NATO, May 20, 2019, https://www.nato.int/cps/en/natolive/topics_69332.htm.
[50] NATO, "Cyber Defence," NATO, July 14, 2022, https://www.nato.int/cps/en/natohq/topics_78170.htm.

Committee/Cyber Defence to "Cyber Defence Committee", and NATO defence ministers tasked NATO to develop a new cyber defence policy, one that would be far wider and extensive, exploring the various aspects of cyber, including legal aspects and considerations, as well as a comprehensive outline regarding relations with the private sector. It was at the NATO 2014 Summit in Wales that this new Enhanced Cyber Defence Policy was approved by NATO Allies and cyber defence was recognized as part of NATO's collective defence, stating that "*[Cyber-attacks] can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence*",[51] as well as the recognition that international law applies in cyberspace.[52] This step changed how cyber defence was perceived within the Alliance and it drastically changes how NATO may respond to cyber-attacks. With cyber defence now a part of NATO's collective defence a cyber-attack on one or more member-states could be grounds to invoke Article 5 of NATO's founding treaty; this is the article that guarantees NATO's collective defence, that in the event of one country being the victim of an attack – or cyber-attack in this case – it would mean an attack on all Allies, and would mean that all Allies would be called to the defence of the attacked Ally, although cyber-attacks would be a "*case-by-case basis.*"[53] In the same year, following the NATO Summit in Wales, and as per NATO's new Enhanced Cyber Defence Policy, the Alliance launched a cooperation initiative with the private sector, called the NATO Industry Cyber Partnership (NICP); through the NICP, NATO can better and more efficiently and effectively reach its goal of cybersecurity by recruiting and working with the private sector. The NICP's initial success was seen at its presentation where there were

[51] "Wales Summit Declaration," *NATO*, September 5, 2014, NATO, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
[52] Ibid.
[53] Ibid.

around 1500 cyber industry leaders as well as policy makers, giving it and NATO-Private Sector a healthy vote of approval.[54]

Since many NATO members are also members of the European Union, the two organizations are inevitably closely tied, and so it stands to reason that it is mutually beneficial to cooperate when it comes to cybersecurity and defence. The European Union is NATO's closest partner when cooperating in these areas, more so than the United Nations, or even the Organization for Security and Co-operation in Europe (OSCE). It recognizes that cybersecurity is a fundamental element of its security, and has intensified its focus in that area accordingly, constituting several entities, such as the EU Agency for Network and Information Security, the European Cybercrime Centre, the European Defence Agency, the European Security and Defence College, and an EU Computer Emergency Response Team. Other relevant steps by the EU to strengthen their cybersecurity are: the adoption of the Directive on Security of Network and Information Systems – a directive that "*seeks to achieve a high common level of security of network and information systems across the EU for a functional internal market*"[55]; the development of the Cyber Diplomacy Toolbox which allows the imposition of sanctions on individuals or organizations to counter potential cyber threats[56]; the implementation of two cyber projects – the Cyber Threats and Incident Response Information Sharing Platform and the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security – under the EU's Permanent Structured Cooperation; and cybersecurity certification for online services and consumer devices[57]. With that in mind, a joint declaration in 2016 between the President of the

[54] NATO, "Cyber Defence," NATO, July 14, 2022, https://www.nato.int/cps/en/natohq/topics_78170.htm.
[55] Susan Davis, *NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE* (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 12.
[56] António Miguel Neves Almeida and Lino Santos, Interview: Coordinator Lino Santos, personal, February 13, 2023. Refer to Appendix III, p. 197.
[57] Susan Davis, *NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE* (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 12.

European Council Donald Tusk, the President of the European Commission Jean-Claude Juncker, and NATO's Secretary General Jens Stoltenberg expanded that cooperation between the two organizations[58]. Also in 2016 NATO's NCIRC (NATO Computer Incident Response Capability) and the EU's CERT-EU (Computer Emergency Response Team of the EU) agreed upon a "Technical Arrangement on Cyber Defence" with the goal of facilitating cooperation with regards to the defence of European cyberspace; ultimately this agreement helps both organizations to coordinate more effectively to prevent or defend against cyber-attacks, and when it comes to sharing practices between teams and the exchange of information. Later in the year the two organizations would also agree on over forty (40) measures to advance how both work together and deal with cyber and hybrid threats; as mentioned earlier, NATO and the EU share the same space and roughly the same priorities, so it stands to reason both would want to strengthen ties, especially when it came to defence, information exchange, and joint research and exercises, in regards to cyberspace, although not solely limited to the latter. At the 2016 NATO Summit in Warsaw, Allies reaffirmed and recognized cyberspace as a domain of operations equal to that of air, land and sea, and that it must be defended just as effectively, improving NATO's ability to conduct operations in that domain. At the same summit, as a matter of priority, NATO Allies agreed to a "Cyber Defence Pledge" to individually strengthen and enhance their national cyber security capabilities as well as its relevant infrastructures, improving their ability to effectively and hastily respond to any cyber-attack.[59] The Allies also welcomed initiatives undertaken in other international forums when it came to sensibilizing and incentivising responsible state behaviour in cyberspace as well as the fostering of confidence-building measures, which promoted a more stable and transparent cyberspace. Following this recognition, defence ministers within NATO approved in 2017 an updated

[58] Ibid., 11.
[59] "Warsaw Summit Communiqué," *NATO*, July 9, 2016, NATO, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

"Cyber Defence Action Plan" as well as a roadmap to make the implementation of cyberspace an operational domain a reality. At the same time NATO strengthen its ties with Finland by signing a Political Framework Arrangement with the Scandinavian country; this agreement would allow for closer cooperation between NATO and Finland to better protect and improve their respective networks. In late 2017 NATO and the European Union took another step in strengthening their cooperation in a number of areas, notably here in regards to cybersecurity and defence; specifically it involves analysis of cyber threats, collaboration between the various NATO-EU incident response teams, good practice orientation regarding cyber aspects, and crisis management orientation.[60] It is worth noting that a according to a 2018 report, the implementation of several NATO-EU cooperation proposals resulted in the "*active, effective interactions and information exchanges between staff, notably on concepts and doctrines; existing training and education courses; threat indicators; threat alerts and assessments; and crisis management*"[61], among which are: the integration of cyber defence in planning, the fostering of cyber research and technology innovation, the exchanging of good practices at the staff level when it comes to crisis management and response, the analysis of threats and malware information, the identification of potential synergies between NATO and the EU, and the strengthening of training exercises.[62]

At the 2018 NATO Summit in Brussels allies took another step to solidify their position in cyberspace by committing to the creation of a new Cyberspace Operations Centre to strengthen NATO's Command Structure; this new Centre would coordinate NATO's cyber operations and other operational activities within cyberspace. Another point that was agreed upon at the 2018 Summit was the ability for NATO to draw on national cyber capabilities for

[60] NATO, "Cyber Defence," NATO, July 14, 2022, https://www.nato.int/cps/en/natohq/topics_78170.htm.
[61] Susan Davis, *NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE* (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 11.
[62] Ibid.

use in their operations and missions.[63] It is worth mentioning that, like other military resources – such as combat vehicles, ships and aircraft – these contributed cyber resources and capabilities would remain in the full ownership of the respective member-state. At the beginning of 2019, Allied defence ministers endorsed a NATO guide that would set out a comprehensive orientation and tools that would further strengthen NATO's ability to respond to any malicious cyber activity. When it comes to defence, the obvious solutions are not enough to counter threats, a wall and weapons are not enough to defend from an attack, it is important to also keep the attack from happening in the first place; this is where the less obvious solutions contribute to defence, these being political and diplomatic tools, tools that can also be used, and must be used, in the defence of cyberspace as well. This guide endorsed by Allied defence ministers does exactly that, it helps NATO and its other Allies to not only enhance their situational awareness within cyberspace, but also to boost their cyber resilience and to work with Allies and partners to deter, defend and/or counter any kind of malicious cyber activity. During the 2021 Summit in Brussels NATO members approved a new Comprehensive Cyber Defence Policy that would better support NATO's three core tasks of collective defence – these being deterrence and defence, crisis prevention and management, and cooperative security. It is stated that the Alliance must "*employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns, in accordance with international law*"[64], meaning that be it in peacetime, crisis, and/or conflict, NATO must be constantly active in its deterrence and defence, and in punishing those who harm the Alliance, be it through cyber resources or outside of cyberspace. Allies at the summit also recognized that a significantly malicious or cumulative cyber-attack, or any other impactful cyber activities, might be considered an armed attack in

[63] "Brussels Summit Declaration," *NATO*, July 11, 2018, NATO, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
[64] "Brussels Summit Communiqué," *NATO*, June 14, 2021, NATO, https://www.nato.int/cps/en/natohq/news_185000.htm.

certain circumstances, leading to the potential invocation of NATO's Article 5. Finally, it was agreed to make greater use of NATO as a political consultation platform among Allies, stating that the Alliance "*will make greater use of NATO as a platform for political consultation among Allies, sharing concerns about malicious cyber activities, and exchanging national approaches and responses, as well as considering possible collective responses.*"[65] This closer interoperability and cooperation ensures that NATO's cyber defences and capabilities can function more effectively when dealing with potential cyber threats. Later in the year NATO's North Atlantic Council appointed Mr. Manfred Boudreaux-Dehmer to be NATO's first Chief Information Officer (CIO); his mission would be to facilitate the integration, alignment and cohesion of NATO's ICT system throughout the entire Alliance.[66]

More recently, during the 2022 NATO Summit in Madrid, one marked by the Russian invasion of Ukraine, allies decided on a few points concerning cyber. Firstly, due to the aforementioned Russian invasion, NATO has decided to offer, among other defence measures, to help fortify Ukraine's cybersecurity and cyber defence capabilities as well as to assist in a levelled integration process of those cyber capabilities to other branches of Ukraine's Armed Forces to guarantee a strengthened and long-term interoperability between all branches of the Ukrainian Armed Forces[67]. As we had mentioned above, today, there is a greater dependency on cyberspace when conducting war and other military operations, to a point where crippling access to cyberspace, or outright disabling access to cyberspace altogether, may seriously hinder the military's ability to conduct its operations or affect operations' success rate, depending on the level of dependency of cyberspace a country's military has; and, as such, it makes a nation's cyberspace a tempting target for the enemy to attack, so therefore, this domain

[65] Ibid.
[66] NATO, "Cyber Defence," NATO, July 14, 2022, https://www.nato.int/cps/en/natohq/topics_78170.htm.
[67] "Madrid Summit Declaration," *NATO*, June 29, 2022, NATO, https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

must be equally protected to the same degree physical military targets and objectives are. Russia is aware of this reality, and that is why a day before and during the first hours of their invasion of Ukraine they conducted a series of cyber-attacks to help cripple Ukraine's defensive response to the invasion. A malware "wiper" software was used in the first hours of the invasion, having been secretly placed within Ukrainian networks three months before the invasion, and activated a day before the invasion began. This scale of the attack inadvertently affected Latvia and Lithuania, NATO member-states, as well[68]. Therefore, it is imperative that these crippling attacks must not be allowed to affect NATO states, and although a Ukraine-NATO partnership already existed with regards to cybersecurity and cyber defence, the Russian invasion changed the paradigm, which necessitated a counterresponse, not only to protect Ukraine's interests, but also to protect NATO interests, and guarantee attacks like these do not spill over onto NATO member-states. Another decision taken during the Madrid Summit was the development of "rapid response" cyber capabilities through the use of national assets. This would increase NATO's ability to respond to a cyber-attack and increase its effectiveness and coordination when responding to an attack[69]. As we have seen, cyber threats can come in many forms, and the scope of an attack, or attacks, may vary, so therefore, the development of rapid response capabilities are invaluable if one intends to halt the spread and the effects of a cyber-attack, especially during these times of war. This follows the European Union's decision to create and implement its own Cyber Rapid Response Teams (CRRT) in May 2021[70], and which were first activated at the request of Ukraine at the start of the Russian invasion.

[68] Frank Bajak, "Cyberattacks Accompany Russian Military Assault on Ukraine," *Associated Press*, February 24, 2022, https://apnews.com/article/russia-ukraine-technology-business-europe-russia-9e9f9e9b52eaf53cf9d8ade0588b661b.

[69] "Madrid Summit Declaration," *NATO*, June 29, 2022, NATO, https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

[70] "CYBER EXERCISE PROVES READINESS TO RESPOND TO CYBER THREATS," *PESCO*, May 28, 2021, European Union, https://www.pesco.europa.eu/wp-content/uploads/2021/05/PRESSSTATEMENT-CRRT.pdf.

Also, important to note is the stance NATO has had in recent years on the state of cyberspace and cyber activities world-wide, most notably regarding malicious cyber activity and its seemingly increasing occurrences. In 2020, during the coronavirus pandemic, a series of cyber-attacks took place targeting research centres and institutes, hospitals, and a varying array of healthcare services essential to combating the spreading pandemic. In the light of these attacks NATO and its NAC issued a statement condemning these cyber-attacks, and expressing support and solidarity to all those affected; it also offered support to the affected parties and called for respect for international law and norms regarding responsible state behaviour in cyberspace.[71] A year later in 2021 the NAC issued a similar statement of solidarity regarding the then recent ransomware attacks and other malicious cyber activities, especially to those affected by the Microsoft Exchange Server compromise. This statement highlighted and condemned the targeting of critical infrastructure and democratic institutions, and the exploitation of supply chain weaknesses while also emphasising the importance of states when it comes to the promotion and the upholding of voluntary norms in responsible state behaviour.[72] Public political stances such as these have been incremental to NATO's continuing affirmation within cyberspace and all matters concerning cyber.[73]

[71] "Statement by the North Atlantic Council Concerning Malicious Cyber Activities," *NATO*, June 3, 2020, NATO, https://www.nato.int/cps/en/natohq/official_texts_176136.htm.
[72] "Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise," *NATO*, July 19, 2021, NATO, https://www.nato.int/cps/en/natohq/news_185863.htm.
[73] NATO, "Cyber Defence," NATO, July 14, 2022, https://www.nato.int/cps/en/natohq/topics_78170.htm.

3. NATO's Approach to Cyberspace Security

Going back to the NATO Parliamentary Assembly's STC's General Report "NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence" we will see, as we already know, that cyber-attacks, due to their ambiguous nature, are a possibility during peacetime; they can be used against NATO by its adversaries, and, likewise, can be used by the Allies against their adversaries.[74]

According to the STC's General Report, "*NATO maintains a cyber deterrence policy of ambiguity*"[75], which essentially means that NATO does not explicitly specify to what point a cyber-attack is sufficiently damaging that it would be considered an armed attack, and therefore, warrant the activation of NATO's Article 5. This level of ambiguity allows NATO a few advantages: firstly, this level of ambiguity draws an invisible line, a line that adversaries will not want to cross, yet, at the same time, do not know how far that line is, and therefore, do not know how far they can go in their cyber-attacks, for fear of Article 5's activation. Were they to know precisely where that line is then they would increase their attacks – both in number and intensity – just below the line, constantly skimming around its edges, never crossing it, knowing full well that it would not constitute an armed attack. Secondly, this ambiguity extends to the type and degree of punishment an adversary would suffer in retaliation for an attack; in other words, NATO does not clarify if it would use the full extent of its capabilities or not in their response to an attack, creating doubt and dissuading adversaries from conducting cyber operations against NATO. Thirdly, due to the frequency of cyber-attacks against NATO, coupled with the lack of international consensus regarding this matter, it would generally be impractical for NATO to activate Article 5 every time a cyber-attack occurred. Fourthly, it

[74] Susan Davis, "NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE" (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 3-4.
[75] Ibid., 7.

allows NATO to conduct its own cyber operations against adversaries, whether they are attacks or pre-emptive attacks described in the "Persistent Engagement" strategy of the United States, a concept of "Defend Forward", a strategy the STC General Report encourages Allies to explore and potentially adopt.[76]

NATO Allies contribute both defensive and offensive cyber capabilities to the Alliance, however, it is important to note that, unlike defensive cyber capabilities, offensive cyber capabilities are not under NATO command and control and are instead under the command and control of the respective contributor Ally[77]. This functions similarly to how other specific forces are employed within the Alliance's operations, such as a nation's special forces. Allies are reluctant to share defensive cyber capabilities with other member-states, and even less so when it comes to offensive cyber capabilities where there is no sharing of any kind whatsoever. When it comes to information, we do see a greater level of sharing between Allies. The integration of these cyber capabilities into the Alliance is done through the Cyberspace Operations Centre located in Mons, Belgium, allowing for a greater coordination of cyber operations, more effective and centralised planning, and providing situational awareness[78]. In practice, this will mean that the aforementioned NCIA, Allied Command Operations (ACO) and the Supreme Allied Commander Europe (SACEUR) will have a closer cooperation relationship. It is, however, important to guarantee, with the integration of cyber assets into NATO's command and control structure, heavy political oversight, as well as strict adherence to international law.[79]

---

[76] Ibid., 7-8.
[77] Ibid., 9.
[78] Sandor Vass, "Panel 2 - Cyber Resilience & Preparedness: Harmonizing Requirements to Delivering Operational Capabilities: Cyberspace Operations Centre - A Capability User Perspective," Academia Militar, 2018, https://academiamilitar.pt/images/site_images/5th_NATO_Cyber_Defence/8_Brigadier_General_HUN_Army_Sandor_VASS_Director_Cyberspace_Operations_Centre_ACO_-_CyOC.pdf, 8.
[79] Susan Davis, "NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE" (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 9.

3.1. NATO's Cyber Institutions and Agencies

The protection of the Alliance's networks and cyber assets is one of NATO's missions, and as such, it does this by way of mutual assistance and information sharing, done through the various military and technical bodies within NATO, such as ACO and Allied Command Transformation (ACT) as well as the NCIA – which provides communications and information systems and delivers communications capabilities and technology according to the Alliance's needs – and the Malware Information Sharing Platform (MISP); education and training, usually done through the NCI Academy, the NATO Defence College, the NATO School in Oberammergau, and the CCDCOE, as well as other Smart Defence projects, such as the Multinational Cyber Defence Education and Training (MN CD E&T), led by Portugal, which includes twenty three (23) member-states and other non-NATO nations, such as Japan (a recent member of the CCDCOE[80]), Macedonia, among others[81], and other entities such the European Union, the NATO Standardization Office (NSO) and the ACO[82]; by conducting exercises, such as the "Cyber Coalition 2022", the establishment of the NATO Cyber Range (CR14) in Estonia to conduct said Cyber Coalition Exercises run by ACT – which involves over 700 participants from member-states, NATO partners and the European Union, and people of industry and academia – and Coalition Warrior Interoperability Exercises (CWIX)[83], as well as exercises run by the CCDCOE, such as "Locked Shields" which tests skills in an intensive two team 1v1 scenario and "Crossed Swords" which allows cyber experts to defend networks against a

[80] Alexander Martin, "Japan Formally Joins NATO Cyber Cooperation Center," *The Record*, November 4, 2022, https://therecord.media/japan-formally-joins-nato-cyber-cooperation-center.
[81] António Miguel Neves Almeida and Paulo Viegas Nunes, Interview: Brigadier General Paulo Viegas Nunes, personal, January 13, 2023. Refer to Appendix I, p. 158.
[82] NATO-MNCDET, ed., "Participants: MNCDET-NATO," MN CD E&T, accessed March 17, 2023, https://mncdet.wixsite.com/mncdet-nato/participants.
[83] NATO-CR14, ed., "Cyber Ranges," CR14, accessed March 15, 2023, https://www.cr14.ee/ranges#nato-cyber-range.

simulated cyber-attack; and by raising and enhancing awareness, by, for example, including cyber threats into NATO's Crisis Management Exercise.[84]

The NCIA is, essentially NATO's technology and cyber experts, and is particularly important when dealing with cyber, dealing with the acquisition of technology, experimentation, testing and technical support, systems and architecture design and engineering, as well as interoperability. It supports the IT needs of NATO HQs, Command Structures and its several Agencies, and, as mentioned above, it provides communications and information systems and delivers communications capabilities and technology according to the Alliance's needs. It manages NATO's Computer Incident Response Capability (NCIRC), a team that provides cyber threat analysis and defends NATO owned and/or operated networks continuously, be they stationary or mobile. Within the NCIRC is its Rapid Reaction Team (RRT), a team composed of a core of six experts that are able to respond to incidents within a window of 24 hours; a team that can be deployed in support of a member-state – upon approval of the North Atlantic Council – and to NATO sites, whether they are in an operational theatre or not. The NCIA also operates a Cyber Security Collaboration Hub where Allies can exchange information, share best practices, and work within an encrypted workspace. The NCIA also operates and Academy, previously mentioned, in Oeiras, Portugal, which trains both civilians and military staff on NATO's advanced IT and cyber systems, and also connects the other training locations in academia, industry, as well as other NATO member-states.[85]

Another, previously mentioned, aspect of the NCIA is its Academy, the NCI Academy, located in Oeiras, Portugal. While it is not an exclusive "cyber" school, it does train students in cyber, with its cyber curriculum deriving, in part, from the MN CD E&T, and the European

[84] Susan Davis, "NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE" (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 9-10.
[85] Ibid., 10.

Union Military Training Group "Cyber Defence Discipline" (EUMTG/CD Discipline), both led by Portugal. The process of launching the cyber curriculum was followed by the NCI Academy's first (acting) Director, Brigadier General Paulo Viegas Nunes, who worked at the previous iteration of the NCI Academy, the NATO Communications and Information Systems School (NCISS), which was based in Latina, Italy, as NCISS Commandant, as well as manager of the MN CD E&T project[86]. The Academy commenced its operations in 2019, and has since been responsible for the dynamic, flexible and adaptive training of both civilian and military personnel, with the capabilities to offer education and training at a distance through e-learning, allowing for greater access to said training and education. The Academy is "*accountable for the provision of Education and Training (E&T) Services to NATO and the Nations. It delivers individual and collective training on NATO Communications and Information Systems, including AirC2, support to the Military Training and Exercise Programme and assistance to NATO and National Commands preparing for NATO operations. The Academy also provides E&T services for [NCI] Agency staff in support of professional and personal development, as well as mission (post)-specific requirements […].*"[87] NATO did not have a cyber curriculum[88], but with the NCI Academy NATO can be provided with a world-class E&T capability, allowing it to keep up with other superpowers, technologically speaking, and has set a goal to train over 10,000 cyber defenders within a period of five years[89]. It has become a game changer, and while it intends to, it does not yet have the ability to conduct a wide array of research or conduct innovative courses, a fact only worsened by the war in Ukraine.[90]

[86] António Miguel Neves Almeida and Paulo Viegas Nunes, Interview: Brigadier General Paulo Viegas Nunes, personal, January 13, 2023. Refer to Appendix I, p. 158.
[87] NCI Agency, ed., "NCI Agency: About the NCI Academy," NCI Agency | About the NCI Academy, accessed January 12, 2023, https://www.ncia.nato.int/what-we-do/nci-academy/about-the-nci-academy.html.
[88] António Miguel Neves Almeida and Paulo Viegas Nunes, Interview: Brigadier General Paulo Viegas Nunes, personal, January 13, 2023. Refer to Appendix I, p. 158.
[89] NCI Agency, ed., "NCI Agency: About the NCI Academy," NCI Agency | About the NCI Academy, accessed January 12, 2023, https://www.ncia.nato.int/what-we-do/nci-academy/about-the-nci-academy.html.
[90] António Miguel Neves Almeida and António Gameiro Marques, Interview: Rear-Admiral António Gameiro Marques, personal, January 23, 2023. Refer to Appendix II, p. 183-4.

3.2. NATO's Cyber-Partnerships

It is not enough to simply be limited to NATO agencies and entities when dealing with our cybersecurity and cyber defence, rather, it is essential, as we have seen multiple times throughout this thesis, that NATO must also rely on its Smart Defence and maintain a strong network of partners to further its goals; this network needs to include other international organizations, as well as partner nations, and must also include both industry and academia. As we shall see throughout this thesis, many nations focus on partnering up with the industry sector as it is one that can provide technical innovation and solutions, as well as having the ability to invest greatly in cybersecurity and defence, in some cases more so than governments. "*Private institutions/organizations that are leaders in creativity, innovation, and entrepreneurship in cyber-security and [defence] work along with NATO to create a resilient and robust protection mechanism against electronic threats.*"[91] It is also important to note that the industry sector operates and/or owns a large part of the Alliance's information systems. Since the industry sector also possesses knowledge and intelligence on cyber threats, the Alliance has created the NATO Industry Cyber Partnership (NICP) to facilitate information sharing and create a forum where NATO member-states, cyber experts, Alliance entities and industry representatives can come together.[92] For NATO to continue to have a resilient cybersecurity and defence it must maintain this partnership between the Alliance and the industry sector and its respective civilian capabilities, which in turn will add value to NATO and ensure economic growth and sustainability.[93]

[91] Marios Panagiotis Efthymiopoulos, "A Cyber-Security Framework for Development, Defense and Innovation at NATO," *Journal of Innovation and Entrepreneurship* 8, no. 1 (2019), https://doi.org/10.1186/s13731-019-0105-z, 1.
[92] Susan Davis, "NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE" (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 11.
[93] Marios Panagiotis Efthymiopoulos, "A Cyber-Security Framework for Development, Defense and Innovation at NATO," *Journal of Innovation and Entrepreneurship* 8, no. 1 (2019), https://doi.org/10.1186/s13731-019-0105-z, 6.

It is also worth mentioning that it is within the best interest of the industry sector to partner up with NATO and respective national governments to tackle the issue of cybersecurity and defence. No private company in the world wants to fall prey to a cyber-attack; such a scenario would prove costly in terms of recovery and would mean a loss of profit if systems were affected for a period of time. Likewise, a nation's armed forces and cyber institutions cannot afford to hold sole responsibility over the cybersecurity and defence of private entities' networks, nor do private entities wish to rely solely on public entities to safeguard their networks. Such a reality would mean an increase in expenses of public money, so it is in the interest of a nation to have its industry sector cooperate in the development and innovation of cybersecurity. Many attacks are directed towards not at government networks and infrastructure, but against private companies, as well as critical infrastructure that may or may not be held and managed by a private entity; and in some cases, national entities use services provided by private entities. An example of the latter can be seen when in February 2022, Vodafone Portugal became the victim of a cyber-attack. The attack disrupted their operations, and the company was unable to provide the vast majority of their services for almost a week; this in turn affected the Portuguese 112 emergency line, which depends partly on Vodafone Portugal's services and infrastructures[94]. We can, therefore, see here how a targeted disruption of service cyber-attack can cause a great impact on a critical element of national infrastructure. Therefore, it is in the best interest of both parties, for both security and economic reasons, to cooperate in finding solutions and innovations within cybersecurity and defence.

When it comes to Academia we will, likewise, see throughout this thesis how important it is, and how it helps keep NATO ahead of other superpower nations, whether it's for training or development of new technologies or methods. Likewise, when it comes to partner nations,

[94] António Miguel Neves Almeida and António Gameiro Marques, Interview: Rear-Admiral António Gameiro Marques, personal, January 23, 2023. Refer to Appendix II, p. 180.

we have seen that many non-NATO countries participate actively with NATO, such as other European nations like Sweden and Finland (now the 31st NATO member-state), or Western-leaning nations, such as Japan, Australia, New Zealand, among others. In terms of cyber-cooperation, NATO has formed a deep partnership with both Georgia and Ukraine. NATO supports Georgia's cyber capabilities, cooperation and interoperability through the Substantial NATO-Georgia Package (SNGP). This Package is composed of "*defence and related security capacity building initiatives. It involves support for all military services and branches, advice and liaison at all levels (strategic, operational, tactical), capacity-building and training activities, and multinational exercises*"[95], where all NATO member-states have contributed. While the SNGP is not strictly limited to cybersecurity and defence, it is one of the sixteen initiatives under the Package, with the aim of expanding Georgia's cyber capabilities and strengthen its cyber defence capacity to be in line with NATO's standards, with support from a NATO team of experts led by Estonia that also provide consistent advice. The SNGP also applies NATO standards and best practices to Georgia's defence sector, as well as implementing cyber training and awareness initiatives for its defence forces and Ministry of Defence while expanding the country's participation in NATO-led cyber exercises, such as the aforementioned Cyber Coalition, or the CCDCOE's Locked Shields. Under the SNGP Georgia has become a full participant of the MISP, and Georgia's Defence Institution Building School has become a partner of NATO's Cyber Defence Initiative, with the goal of establishing a Cyber Security and Information Technology Study Programme to address both civil and military professionals' lacking knowhow. The Cyber Defence Initiative also foresees the creation of a Cyber Lab in Georgia, a project led by the Netherlands with the objective of enhancing Georgia's overall cyber capabilities.[96] Likewise, NATO supports Ukraine in a

[95] NATO, ed., "The Substantial NATO-Georgia Package," NATO, February 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/2/pdf/Cyber-Defence-georgia.pdf.
[96] NATO, ed., "The Substantial NATO-Georgia Package," NATO, February 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/2/pdf/Cyber-Defence-georgia.pdf.

similar fashion through a Trust Fund on Cyber Defence for Ukraine, which is led Romania (acting through its intelligence service) and RASIROM R.A. (as Executing Agent), and includes the USA, Turkey, Albania, Estonia and Portugal, among others, as contributors. The Trust Fund provides Ukraine with purely defensive capabilities, including Cyber Security Incident Response Team-type technical capabilities – Incident Management Centres – and cyber forensic labs to investigate cybersecurity incidents, providing an integrated system for cybersecurity and defence. The Trust Fund, similar to the SNGP, has to it an advisory dimension and provides training and exercises to Ukraine's cyber experts.[97] Another element of the Fund is to provide a framework that will allow Ukraine to develop its cyber defence through its own national efforts. The plan also foresees, in the long run, keeping the organizational format of the Fund and the raising of more contributions to develop the project, as well as the possibility of securing more Critical Information Infrastructures for Ukraine and delivering more training courses.[98] All this has the possibility of being scaled, depending on the funds available and Ukrainian needs.[99] More recently, Ukraine entered into an agreement to become a member of the CCDCOE,[100] and by mid-2023, it was officially accepted,[101] thereby strengthening the country's defence cooperation with NATO.

[97] Miruna-Maria Cocolan, "International Cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence," *International Cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence* (2018), https://www.cipre-expo.com/wp-content/uploads/2018/10/Cocolan%20M%20NATO-UKRAINE%20Trust%20Fund%20on%20Cyber%20Defence.pdf, 7.
[98] Ibid., 8.
[99] NATO, ed., "UKRAINE Cyber Defence - NATO Trust Fund," NATO, June 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf.
[100] Daryna Antoniuk, "Ukraine Signs Agreement to Join NATO Cyber Defense Center," *The Record*, January 20, 2023, https://therecord.media/ukraine-signs-agreement-to-join-nato-cyber-defense-center.
[101] The Defense Post, "Ukraine Joins NATO Cyber-Defense Center," *The Defense Post*, May 17, 2023, https://www.thedefensepost.com/2023/05/17/ukraine-joins-nato-cyber-defense/.

PAGE LEFT INTENTIONALLY BLANK

4. The Different Approaches to Cyberspace Security within NATO

While NATO is composed of thirty-one (31) member-states – each with a different cyber strategy – it encourages Allies, as part of the Cyber Defence Pledge, to prioritise the cyber security and defence of their national networks and infrastructures. This is the sole responsibility of each Ally to develop its individual capabilities, and, as a result, the collective capabilities.[102] There are seven main objectives they must pursue, according to the Cyber Defence Pledge: "*Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks; […] Allocate adequate resources nationally to strengthen our cyber defence capabilities; […] Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices; […] Improve our understanding of cyber threats, including the sharing of information and assessments; […] Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences; […] Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance; […] Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends.*"[103]

Although we talk of NATO as a whole, we must look at key NATO member-states for some examples of how they approach cyber, cyber defence and cybersecurity, because it is

[102] Susan Davis, *NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE* (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 8.
[103] "Cyber Defence Pledge," *NATO*, July 8, 2016, NATO, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

through individual states that a basis of cooperative defence is constructed, leading to the most effective solutions being implemented in that defence solution. As NATO consists of thirty-one (31) sovereign member-states, each has a different approach to how the deal with cyber threats. This can be due to their cyber capabilities, their understanding of what cyber defence and cybersecurity is, and it may be due to their legislative and executive protocols when it comes to decision-making and concerning deployment of their armed forces and other defensive measures; it can also be due to the fact that some member-states are simply more organized in applying their cyber capabilities more effectively when it comes to dealing with cyber threats, having cyber – or certain aspects of it – allocated to specific ministries, offices, in some cases sharing heads with intelligence departments. Cyber may also be allocated to national armed forces too, with some states having created specific cyber commands or centres to more effectively deal with potential cyber threats.[104]

Security, and by extent cybersecurity, must be based on legal norms and principles that must be acceptable to the wider international community, so therefore, we will look at general aspects regarding the legal and institutional framework of different NATO member-states. This includes rules, rights, and obligations set out in nations' constitutions as well as legislation, policy, regulations and contracts when it comes to a legal framework, and when it comes to institutional framework there are specific laws or provisions that outline national entities' direction. A CCDCOE comparative study on NATO member-states outlines the most regulated and the least regulated areas of cyber-related concepts out of twelve sampled NATO member-states, these being: Cybersecurity, Cyber Defence, Information Security, Information Assurance, Hybrid Threats, and the protection of critical infrastructure. The regulations can either be through legal or policy documents, or through specific strategy outlines. Now, out of

[104] Damjan Štrucl, "Comparative Study on the Cyber Defence of NATO Member States," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2021, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf, 51-2.

these six cyber-related concepts, the most formally regulated are Cybersecurity, Cyber Defence, and Critical Infrastructure Protection, or CIP, with all twelve states analysed having adopted a cybersecurity strategy and only seven of these having adopted a cyber defence strategy; four of these twelve implement a dedicated CIP strategy. The least formally regulated cyber-related concepts are then Information Security, Information Assurance and Hybrid Threats. We can visualize this in *Figure 1*[105], a graph that was taken from the CCDCOE study.

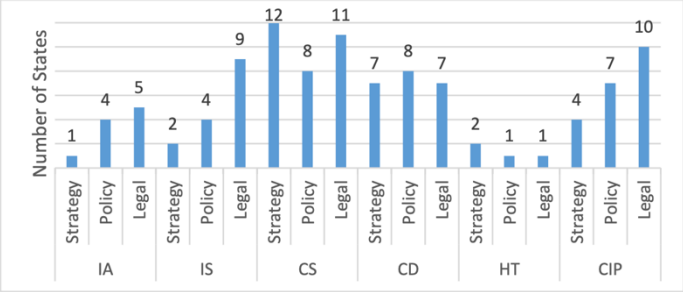

Figure 1: Overview of how States regulate each cyber-related concept.

The reason for this is due to the fact that some countries regulate their entities differently and in some cases group certain concepts together either for practical and efficient reasons or because they see those certain concepts as being a sub-part of a bigger concept or of a different concept, for example how some countries see information assurance as part of information security, and so therefore regulate both as a whole instead of individually. Many NATO member-states are also members of the European Union and so end up transposing EU regulations into their national legislation, such as the EU Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR). For a measurement of quality, quantity, value and extent States apply certain standards, which can be national, such as the US National Institute of Standards and Technology (NIST), or international standards, such as the EU Impact Assessment Steering Groups and NATO Vulnerability Assessments and Penetration tests, or standards from the International Organization for Standardization (ISO). According to the CCDCOE study, most states apply national standards followed by ISO

[105] Ibid., 44.

standards and finally the aforementioned EU and NATO standards. It is important to note that when it comes to cyber defence, most States opted to apply NATO standards.[106]

When it comes to organizational framework, the CCDCOE study states that "*the security of a state depends on several different stakeholders and their roles, […] [a]s a result, states have developed different organisational frameworks that consist of an organisation's structural components and their internal and external interactions*"[107]. These organizational frameworks can either be structured in a centralised or decentralised fashion, each with their own objectives. The study also outlines that the organizational framework should follow a four-levelled top-down model (as seen in *Figure 2*[108]), starting at the policy level, which defines long term political objectives; going down to the strategic level, which sets up organizations or offices to achieve predefined objectives; following that we have the operational, which coordinates the individual and specific tasks within said organizations or offices; and finally at the bottom, the tactical level which deals with the specific procedures when dealing with the aforementioned tasks. The first two levels are responsible for analysing the situation of a state's national security and the development of a national cybersecurity and cyber defence framework; the third level (operational level) focuses on the implementation of those cybersecurity and cyber defence policies; and the final level executes those policies effectively.[109]

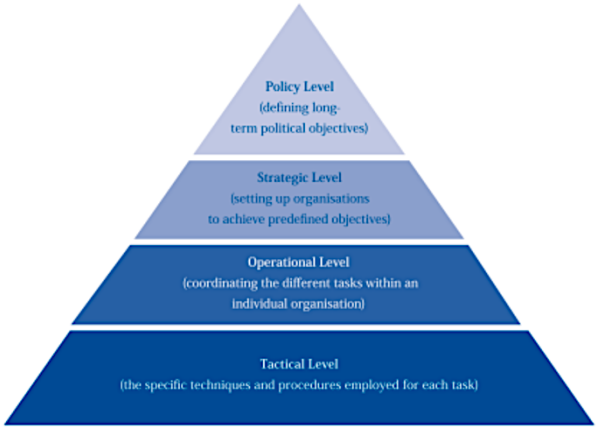

Figure 2: Four-levelled organizational framework.

[106] Ibid.
[107] Ibid., 45-6.
[108] Ibid., 46.
[109] Ibid.

As mentioned above, some states group certain cyber-related concepts, having them administered in the same directorate, office or entity. This means that in some cases there will be states that have one entity that oversees both information assurance and information security, while others might have information security distributed throughout several ministries; five states, for example, have, within their national information security, an intelligence service. When it comes to cybersecurity, most states have attributed that responsibility to the government or a governmental body, such as an agency, to handle it; or it is handled by a specific ministry, such as a Ministry of Defence, Ministry of the Interior, Ministry of Foreign Affairs, or a specific ministry responsible for all national ICT; we can see this in *Figure 3*[110]. When it comes to critical infrastructure protection, the study shows that there seems to be a consensus whereas it is handled by a specific governmental entity, but in some cases these entities serve a more liaison/intermediary or coordinating role between other entities, with some including the national armed forces or their respective Ministry of Defence in their critical infrastructure protection. It is important to note that within cybersecurity all states follow the multi-levelled approach seen in *Figure 2*. When it comes to cyber defence, it is more commonly dealt with by either a State's nationals Ministry of Defence and/or its National Armed Forces, with four of these States having created National Cybersecurity Centres, National Cyber Forces, Cyber Force Commands and Cyber Defence Centres that may in some cases be an independent entity or may be a part of another entity, such as intelligence services. It is important to note that, while cyber defence may be handled by respective national ministries of Defence and/or its

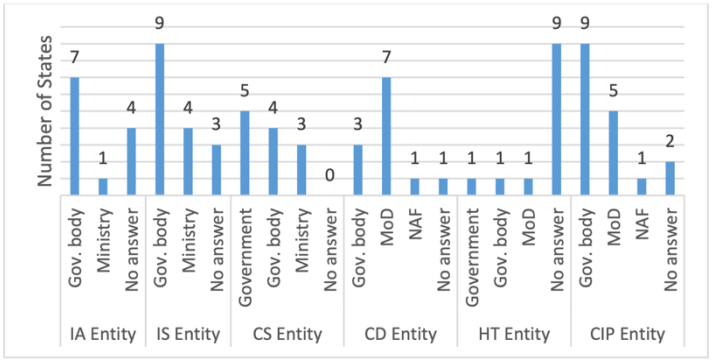

Figure 3: How States divide their cyber-related concepts.

[110] Ibid., 47.

national armed forces, some efforts are joint and operate as such, meaning that it may be done by these two aforementioned entities or may include other entities as well, such as a potential ministry that deals with national ICT or other intelligence agencies/entities. When it comes to both cyber defence and cybersecurity most member-states have centralised as well as dedicated bodies for the dealing of these two points, as seen in *Figure 4*[111]. As we can see, when it comes to cyber defence, the dedicated body here is the Ministry of Defence, and subordinate entities such as national armed forces; but we can see that the same Ministry of Defence is not the dedicated body when it comes to cybersecurity, and is left to specific entities or is centralised

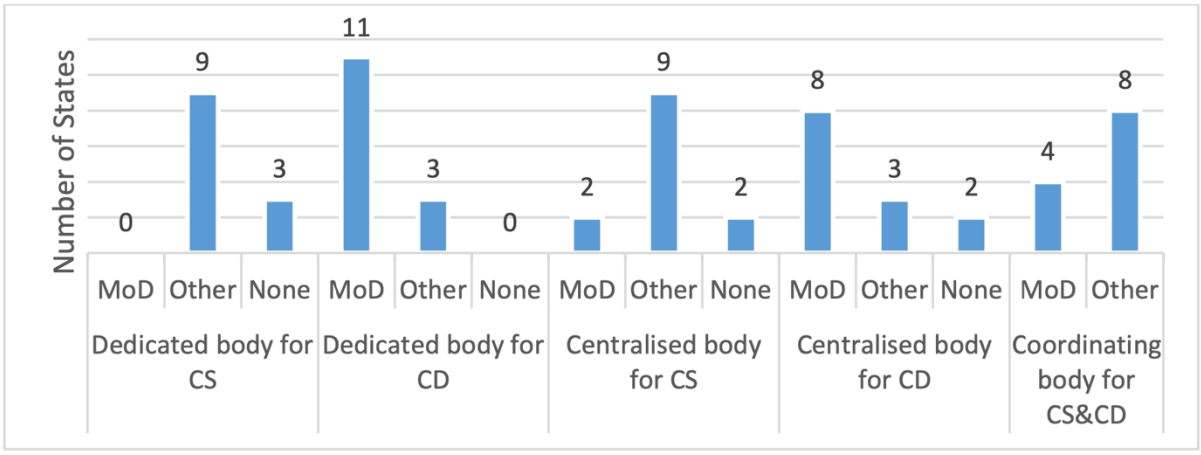

Figure 4: An overview of member-states' government bodies on Cybersecurity and Cyber Defence.

within other ministries or a national Ministry of Defence, and when it comes to centralising or coordinating, most member-states rely on their Ministry of Defence for that duty, as well as when it comes to crisis response.[112] Another aspect to take into account is information sharing and other forms of collaboration, where member-states cooperate with each other, either bilaterally or multilaterally, or through entities such as the European Union, and the United Nations, or, more importantly, through NATO. Information sharing, as well as other forms of cooperation is essential to guaranteeing an effective cybersecurity due to different approaches and methods, as well as capabilities, that we have already seen in this chapter, and as we will

[111] Ibid., 50.
[112] Ibid., 49.

see further ahead when we examine individual examples of NATO member-states and their approaches and procedures. Information that is usually shared consists essentially of either technical or intelligence information. The private sector, as well as academia, is also another method of collaboration, allowing for the development of better and more effective methods and cyber capabilities, something else we will see further ahead.[113]

When we talk about capabilities, we mean having not only possessing the means and resources to carry out cyber operations and cyber defence, but also to have the skills and manpower and knowledge to guide those means and resources in the right direction and in the most efficient way. Many member-states do have these capabilities – as we will see further ahead – but others do not, or at least their capabilities are subpar and can in some cases be considered outdated or obsolete. This is particularly important as a weak defence in one sector – in this case a member-state – could mean a backdoor into NATO's network. To counter this, states within NATO have begun, or are planning to, invest and build future cyber capabilities within the defence sector, with some member-states already possessing offensive cyber capabilities, as we shall also see further ahead. Cyber capabilities are only as good as the people operating them, so therefore, knowledge and skills, and overall human resources are an integral part of cyber capabilities. In that regard, it is important to be able to attract and recruit, as well as retain the acquired human capital to maintain an optimal level of cybersecurity and defence; people are not machines that can be permanently kept and allocated, thus efforts must be made to maintain said human capital. This can be done through incentive programs or rewards and promotions systems, it can be done by guaranteeing free education and training in that area, through decent wages, or an overall positive work environment for employees. As mentioned above, cyber capabilities are only as good as the people operating them, which means a decent level of training is required to guarantee optimal defence capabilities. Training employees will

[113] Ibid., 57.

vary from state to state, this includes the hours of training required as well as the means to train employees. For example, the amount of training and education required – time-wise – can range from 120 hours to six months, and it can be done on-site, or it can be outsourced. Some member-states keep training and education on-site, but may also combine it with outsourcing, sending specialists to either national or international institutions such as foreign or domestic universities, think tank organizations such as CISCO, CompTIA, Palo Alto, and Microsoft, or to specific NATO and European Union sites such as the NCI (NATO Communications and Information) Academy, the NATO School Oberammergau, the CCDCOE, and the European Union Agency for Cybersecurity (ENISA). Training and education are also done through the use of international and national exercises which can be bilaterally organized or may be conducted by NATO, the EU or CCDCOE; exercises include the Cyber Coalition, Crossed Swords, NATO CMX, and Cyber Europe, and may take place annually, biannually, or circumstantially.[114]

We will look at a few examples of specific countries that have a more proactive approach when dealing with cyber threats and examples of countries that prefer a more defensive and passive approach in their cyber defence. The countries in question are the United States, the United Kingdom, France, Germany, Spain, and Portugal. The first three countries have a more proactive and aggressive approach to their cyber defence, while the latter three, focus on a more defensive and reaction-based defence. As mentioned at the beginning of this chapter, nations have different ways of handling their cybersecurity and defence; this can be due to legislative and legal reasons, or it can be due to each nation's cyber capabilities – their quantity and quality – and how effectively they are applied. It is important to understand the perspective and methodology of different NATO member-states since different types of responses as well as procedures can mean a faster or slower response time in that country, and

[114] Ibid., 54-5.

for NATO in general. With the lack of a common approach when it comes to cyber defence and security divisions between those countries that are more active in their cyber defence strategy and those countries that rely on a reaction-based defence strategy may arise. As mentioned above, NATO recently decided to create rapid-response capabilities, to mitigate additional damage caused by longer response times of some member-states. While these rapid-response teams rely on national cyber capabilities, this is not synonymous to having a common approach to cyber defence, therefore, it is essential to understand the different approaches from a sample of NATO member-states, so that we may comprehend why no common approach to cyber defence exist, yet.

4.1. United States of America

We will begin by looking at NATO's core member-state, the United States of America. With a National Cyber Security Index of 64.94,[115] they are by far the largest contributors to the alliance, and their stance, policy, and methodology on key topics generally influences the rest of the alliance and how it operates and conducts itself as a whole, so looking at the United States is imperative.

In 2009 a new Cyber Command (USCYBERCOM) was established within the Strategic Command structure. Aside from its director, the leadership and service elements of USCYBERCOM is composed of three-star cyber command representatives of the four branches of the U.S. Armed Forces; these include: the Army Cyber Command (ARCYBER), US Fleet Cyber Command 10th Fleet (FCC/C10F), US Marine Corps Forces Cyberspace (MARFORCYBER), Coast Guard Cyber Command (CGCYBER),[116] and 16th Air Force

[115] NCSI, "United States," National Cyber Security Index, accessed September 3, 2022, https://ncsi.ega.ee/country/us/.
[116] Piret Pernik, Jesse Wojtkowiak, and Alexander Verschoor-Kirss, "National Cyber Security Organisation: UNITED STATES," CCDCOE, 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf, 20.

(AFCYBER)[117]. Its objective was to guarantee the Pentagon's network was defended, and to ensure greater efficiency and synergy, the director of the new Cyber Command back then was also the director of the National Security Agency (NSA). The U.S. however saw that this was not an effective strategy, realizing that the intrinsicality of cyberspace made it a major battleground with major powers such as China and Russia and other relevant cyber powers such as North Korea, Iran, and other terrorist organizations and groups such as the Islamic State of Iraq and Syria (ISIS). The best metaphor to explain the Cyber Command's initial strategy would be the equivalent of manning a single castle's defences rather than manning the defences of a country's borders; or to put into a more contemporary metaphorical, albeit slightly different, circumstantially speaking, setting: "*it is as if the US Navy had remained in American harbours during the Cold War, waiting for Soviet submarines and ships to arrive, instead of patrolling the Atlantic and the Pacific Oceans to ensure sea routes*"[118]. A turning point for cybersecurity and defence in the United States was after the cyber-attacks of the 2016 presidential race and elections, as well as other cyber-attacks in 2017. The United States perceived the success of these cyber-attacks to be unacceptable for a superpower and its defences. Due to these turn of events, Cyber Command drew a new and more ambitious strategic concept that intended to achieve and maintain cyberspace superiority to "*influence adversary [behaviour], deliver strategic and operational advantages for the Joint Force, and defend and advance [U.S.] national interests*"[119]. This superiority is achieved through the strategy of "Persistent Engagement"[120], in other words, through constant, proactive offensive

[117] USCYBERCOM, ed., "Our Service Cyber Partners," U.S. Cyber Command, accessed September 27, 2022, https://www.cybercom.mil/Components/.
[118] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 11.
[119] United States Cyber Command, Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command § (2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf, 5.
[120] Susan Davis, *NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE* (London, United Kingdom: NATO Parliamentary Assembly's Science and Technology Committee (STC), 2019), 4.

operations, constantly engaging adversaries relentlessly, denying them any opportunity or operational advantage to engage in cyber-attacks against the United States, whilst creating advantages for the Americans. This form of "defence forward" is already in play in other domains of conflict, in air, land, and sea, and the objective with this strategic concept is to implement it into cyberspace as well. It is the view of the U.S. Department of Defence that a more defensive posture, rather than a more offensive posture – and therefore limiting cyber defence to responding to cyber-attacks – will be equivalent to constantly yielding ground to adversaries, leading to the erosion of military power while risking the impairment of national networks as well as encouraging foreign hostile powers to deliver increasingly sophisticated cyber-attacks, with ever rising occurrences. Within the United States, cyber-attacks are kept under the threshold of "armed attacks" due to how frequent and regular such attacks happen against American networks. Were it not kept below that threshold, it would warrant a military mobilization and response from U.S. Armed Forces; while responding to a cyber-attack in such a manner is not impossible, it would however be highly impractical, and would raise several questions and even doubts from the public, especially since cyber-attacks are "invisible" and physical attacks are much easier to perceive. The United States has hence with adopted an offensive strategy in their cybersecurity policy; it involves actively and pre-emptively striking against adversaries that may pose a cyber threat against the U.S., damaging their systems and hindering their capabilities, giving them no opening to strike at the U.S., and forcing them to focus on their own cyber defence, ultimately deterring them from any cyber operations against the U.S. or from responding to cyber-attacks.[121]

To more effectively achieve their goals, the USCYBERCOM follows five "imperatives", or objectives, each one building on the last to guarantee cyberspace superiority.

[121] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 11.

They are as follows: "*[1] Achieve and sustain overmatch of adversary capabilities; [2] Create cyberspace advantages to enhance operations in all domains; [3] Create information advantages to support operational outcomes and achieve strategic impact; [4] Operationalise the battlespace for agile and responsive [manoeuvre]; [5] Expand, deepen, and operationalise partnerships.*"[122] The first of these "imperatives" relies on the identification and anticipation of technological changes to better understand and use them, and to be able to quickly exploit these new technologies, operationalizing them more effectively – by rapidly transferring these technologies that may have military utility to scalable operational capabilities – and quickly, ideally, before adversaries of the United States. The second "imperative" focuses on the development of advantages prior to joint operations in conflict and the integration of cyberspace capabilities and forces into plans and operations across all domains of conflict. The third "imperative" concerns the integration and unification of intelligence capabilities to support cyberspace operations and information operations to improve mission outcomes. The penultimate "imperative" is essential to guaranteeing quick responses to cyber-attacks and one that differentiates member-states and their response time and consequently their overall cyber policy. It focuses on facilitating speed and agility when it comes to policy guidance and decision-making processes, as well as streamlining investment. It also certifies that all aspects of cyberspace operations, or operations where cyber is also involved – such as target system analysis, battle damage assessment, requirements identification, fielded solutions, and so forth – are aligned to the cyberspace operational environment. The fifth and final "imperative" expands on the benefits of cooperating with the private sector, other American agencies, academia and allies. This would allow for a faster identification and understanding of cyberspace advances, complementing with "imperative" one. It would also promote

[122] United States Cyber Command, Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command § (2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf, 8-9.

information sharing between the two allowing for a more streamlined threat analysis as well as more effective capability development. Operational planning, and joint exercises could also solidify cybersecurity capabilities for both parties.[123] It worth noting that the former Secretary of Defence, Mark Esper, has stressed the need for closer interoperability with allies – i.e., NATO – when it comes to developing a combined cybersecurity policy against adversaries such as China and Russia. This sort of policy would allow the United States access to allied networks and systems and to conduct cyber operations using those same systems and capabilities.[124] However, this sort of free access agreement between allies seems unlikely to happen anytime in the near future.

The current (2023) U.S. National Cybersecurity Strategy divides itself in five pillars, each focusing on specific issues and challenges the U.S. wishes to focus on and tackle. These are: (Pillar One) Defend Critical Infrastructure, (Pillar Two) Disrupt and Dismantle Threat Actors, (Pillar Three) Shape Market Forces to Drive Security and Resilience, (Pillar Four) Invest in a Resilient Future, and (Pillar Five) Forge International Partnerships to Pursue Shared Goals.[125]

The first pillar focuses on Critical Infrastructure Protection (CIP) and emphasise the need to have its national critical infrastructure well protected. The importance of this particular topic will be explored further ahead in this thesis. One of the solutions would be through the implementation of cybersecurity requirements and regulations in critical sectors. Regulations would be performance-based, leveraging existing cybersecurity frameworks, voluntary consensus standards, and guidance from organizations like the Cybersecurity and Infrastructure

[123] Ibid.
[124] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 13.
[125] The White House, National Cybersecurity Strategy § (2023), https://www.cybercom.mil/Portals/56/Documents/Mission%20and%20Vision/National-Cybersecurity-Strategy-2023.pdf.

Security Agency (CISA) and NIST. They would be adaptable to evolving adversary tactics and focus on secure-by-design principles, availability of essential services, and be able to quickly recover from failures. Likewise, the strategy seeks to streamline new and existing regulations. According to the strategy, "*[e]ffective regulations minimize the cost and burden of compliance, enabling organizations to invest resources in building resilience and defending their systems and assets. By leveraging existing international standards in a manner consistent with current policy and law, regulatory agencies can minimize the burden of unique requirements and reduce the need for regulatory harmonization*."[126] Scaling public and private collaboration is another solution the U.S. seeks to achieve pillar one. Collaboration would be strengthened through structured roles and responsibilities, facilitated by increased connectivity and automated data exchange. In practice this translates to coordination between infrastructure owners and operators nationwide, and CISA, working alongside Sector Risk Management Agencies (SRMAs), with the Federal Government investing in SRMA capabilities. This collaboration also includes the human-to-human collaboration which would be complemented with machine-to-machine data sharing and security orchestration, enabling real-time and actionable threat response. A third solution to accomplish this pillar is enhancing the integration of the numerous federal cybersecurity centres. The strategy state: "*Operational collaboration models at SRMAs, such as the Department of Energy (DOE)'s Energy Threat Analysis Center (ETAC) pilot, DoD's Defense Industrial Base Collaborative Information Sharing Environment (DCISE), and the National Security Agency (NSA)'s Cybersecurity Collaboration Center provide opportunities to enable timely, actionable, and relevant information sharing directly with private sector partners in their respective sectors.*"[127] Similarly, other bodies were given new or additional powers to better fulfil their mission, such

[126] Ibid., 9.
[127] Ibid., 11.

as the National Cyber Investigative Joint Task Force (NCIJTF) when it comes to cooperation with law enforcement, and the Cyber Threat Intelligence Integration Centre (CTIIC) when coordinating intelligence collection efforts. A fourth solution includes updating the Federal incident response plans, such as the National Cyber Incident Response Plan (NCIRP), and that Acts, such as the 2022 Act of Cyber Incident Reporting for Critical Infrastructure (CIRCIA) are enhanced to more effectively respond to incidents. The final solution involves modernizing Federal defences; for example, securing Federal civilian executive branch agencies, as well as national security systems, through collective operational defence, and by modernizing Federal systems and replacing or updating old systems.[128]

Pillar two exemplifies the United States' more active and offensive approach to cybersecurity and defence. According to the cybersecurity strategy, the United States is committed to using its national resources – cyber or otherwise – to disrupt and dismantle threat actors that pose a risk to its interests. This approach would involve integrating diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities, with ultimate objective of rendering malicious actors incapable of executing sustained cyber campaigns that could jeopardize the United States' national security. One of the methods to achieve this is by increasing and intensifying Federal disruption activities through the NCIJTF, and by developing "*technological and organizational platforms that enable continuous, coordinated operations*"[129], with the ultimate objective of rendering cyber-crime unprofitable and altering foreign governments' perception of conducting cyber operations on the U.S. as an ineffective means to accomplish their goals. The strategy also foresees enhanced cooperation between the public and the private sector in this regard, as well as the increase and enhancement of intelligence sharing. As we shall see throughout this thesis,

[128] Ibid., 7-13.
[129] Ibid., 15.

the private sector possesses and increased importance when it comes to dealing with cyber threats. The strategy argues that the private sector has a growing awareness of adversary activity, often surpassing the Federal Government in breadth and depth of knowledge. This is attributed to the size of the private sector, its proactive threat hunting operations, and the rapid innovation in tools and capabilities, making public-private cooperation – and operational collaboration hubs such as the National Cyber-Forensics and Training Alliance (NCFTA) – essential when conducting disruptive cyber operations. Likewise, the prompt exchange of threat intelligence between Federal and non-Federal partners strengthens collaborative endeavours to disrupt and dismantle adversaries; therefore, the strategy states that "*SRMAs, in coordination with CISA, law enforcement agencies, and the CTIIC, will identify intelligence needs and priorities within their sector and develop processes to share warnings, technical indicators, threat context, and other relevant information with both government and non-government partners*."[130] Another element of the second pillar is to counter and defeat ransomware by leveraging international cooperation, investigate ransomware incidents, bolter resilience within the nation's critical infrastructure, and addressing the use of virtual currency in laundering ransom payments from ransomware.[131]

As mentioned in the second pillar, the third pillar builds on public-private sector cooperation, specifically when it comes to shaping the market. Since many businesses hold clients' personal data, and therefore should hold responsibility for guaranteeing that that data is secure from would-be hostile cyber actors; this is especially so when it comes to health and geolocation information. Similarly, we know that many devices today are increasingly interconnected (an issue that will be touched on further ahead), therefore, it stands to reason that these devices should, likewise, be equally protected. These devices can be computers and

[130] Ibid., 16.
[131] Ibid., 14-8.

phones, exercise trackers, and even home and baby monitors to software and hardware that manage critical infrastructure; the strategy seeks to develop new forms of protection as well as incentivise private companies to do the same. Furthermore, as we shall see further ahead, many private entities and companies forego the implementation of decent security and best practices in the attempt to increase profit margins; therefore, the strategy seeks to shift the liability for insecure hardware and software in the event of failure. Pillar Three also seeks to use Federal grants and other incentives to offer investment opportunities on research and development, as well as leveraging Federal procurement to help improve cybersecurity, such as through the Civil Cyber-Fraud Initiatives (CCFI).[132]

Similarly, the fourth pillar outlines the need to invest in a digital future so as to be able to stay ahead of competing and rival nations, so that "*the United States will maintain its leading role as the world's foremost innovator in secure and resilient next-generation technologies and infrastructure*."[133] This investment intends to address the myriad of foundational vulnerabilities within the Internet, as well as the security challenges facing it, such as unencrypted DNS requests; therefore the U.S. intends to build on public-private sector cooperation as well as partnerships with stakeholders to develop and adopt solutions for these problems, including supporting non-governmental Standards Developing Organizations (SDOs). As mentioned before, Pillar Four's investment objectives focus on research and development, supported by Federal R&D entities, such as the National Science Foundation (NSF) and the Department of Energy. This R&D would proactively address one of the impending risks of the future, namely quantum computing, which possesses the ability to undermine current encryption techniques employed by contemporary hardware and software.[134] Finally, the fourth pillar seeks to, as we will see in many other national

[132] Ibid., 19-22.
[133] Ibid., 23.
[134] Ibid., 23-5.

cybersecurity strategies, strengthen and increase access to cyber education and training for its national workforce, implementing the National Cyber Workforce and Education Strategy.[135]

Pillar Five seeks to build on partnerships, for example on alliances and mechanisms such as NATO, which includes assisting and supporting less capable allied nations that have difficulties or are incapable of investigating, recovering, and/or responding to cyber incidents and attacks, as well as many other partnerships such the Declaration for the Future of the Internet (DFI), which includes over sixty nations; the Quadrilateral Security Dialogue, which includes the U.S., India, Japan and Australia; the Indo-Pacific Economic Framework for Prosperity (IPEF); the Americas Partnership for Economic Prosperity (APEP); The U.S.-EU Trade and Technology Council (TTC); AUKUS, a trilateral security pact between Australia (A), the United Kingdom (UK), and the United States (US); multistakeholder partnerships such as Freedom Online Coalition and Counter-Ransomware Initiative; and the European Cybercrime Centre. Likewise, to support these goals, this pillar intends to strengthen the capacity of the U.S. and its allies by leveraging expertise from the public and private sectors, regional partners, as well as its various agencies, such as the United States Department of Justice, which would engage robust cybercrime cooperation through the several bilateral and multilateral partnerships; the Department of Defence, which would "*strengthen its military-to-military relationships to leverage allies' and partners' unique skills and perspectives while building their capacity*;"[136] and the Department of State, which would ensure the alignment of Federal capacity building and interests with U.S. allied nations, such as through a NATO effort to develop a "*cyber incident support capability that enables Allies to more effectively and efficiently support each other in response to significant malicious cyber activities*."[137] Moreover, through collaboration with the aforementioned alliances, mechanisms, and

[135] Ibid., 27.
[136] Ibid., 31.
[137] Ibid., 31-2.

additional partnerships such as the Indo-Pacific Economic Framework and the Quad Critical and Emerging Technology Working Group, efforts will be made to ensure the integrity and safety of global supply chains for ICT products and services. This includes establishing a transparent and secure 5G network, contributing to the overall goal of building trustworthy and reliable infrastructure, while limiting ICTs and services that are subject to influence or control from foreign powers, such as China. Initiatives such as these are also foreseen to be accelerated by the newly created International Technology Security and Innovation Fund.[138]

This strategy highlights the proactive stance adopted by the United States, serving as a prime example of an offensive cybersecurity approach in action. By actively identifying and addressing potential threats, collaborating with various stakeholders, and promoting the development of secure and resilient infrastructure, the United States sets an example for other nations. This proactive stance enables the nation to stay ahead of emerging cyber threats, effectively mitigating risks and ensuring the protection of critical systems and data.

4.2. United Kingdom

As mentioned above, the United Kingdom – with a National Cyber Security Index of 89.61[139] – and the United States have very similar approaches when it comes to their cybersecurity and cyber defence. Like the United States, the UK focuses on an active and offensive approach to cybersecurity, giving potential adversaries no quarter. Since 2009 the United Kingdom has adopted a centralised approach to its cyber defences and has since developed and invested greatly in the development of cyber capabilities, be it defensive or offensive. On May 2013, to keep up with the developing world of cyber, the UK created the Joint Forces Cyber Group (JFCyG) which was composed of two joint cyber units, one at the

[138] Ibid., 29-33.
[139] NCSI, "United Kingdom," National Cyber Security Index, accessed September 3, 2022, https://ncsi.ega.ee/country/gb/.

Government Communications Headquarters (GCHQ) in Cheltenham, and another at the Ministry of Defence (MoD) Corsham; it is also supported by a Joint Cyber Reserve Force in the form of the Royal Navy Reserve and the British Army Reserve. This Joint Forces Cyber Group is coordinated by the British Ministry of Defence and the aforementioned Government Communications Headquarters (GCHQ). The latter is responsible for coordinating all cyber warfare operations and providing signal intelligence and other information assurances to the UK government and armed forces. In 2016, a new National Cyber Security Strategy was issued; this new national strategy would focus on three key objectives: to defend, deter and develop.[140]

The first is centred around the ability to defend the United Kingdom's networks, assets, and overall cyberspace, be it military, or civilian, increasing defence capabilities and network resilience; these networks and assets include its institutions, economic sector, as well as individual citizens' personal and private data; it is worth noting that the protection of these key administrative networks and also the protection of important companies and organizations are essential to keeping the United Kingdom as a whole stable and secure in the event of cyber-attacks or threats. This is done through what the UK Government calls "Active Cyber Defence", or "ACD", which, as the name implies, involves actively engaging potential adversaries so as to limit their openings and opportunities. This objective also involves scaling up the United Kingdom's cyber capabilities to be able to disrupt serious state sponsored cyber threats; this translates increasing the scale and development of the GCHQ, the Ministry of Defence, and the National Crime Agency (NCA) and its capabilities, including investing in each sectors' programmes. One of the approaches to achieving this objective is to work with industry and the private sector, more specifically sectors that have to do with communications and cyber industry, mainly to keep cyber-attacks away from internet services or to at least to

[140] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 13-4.

reduce the likelihood those cyber-attacks will have a sustained impact on the United Kingdom. The UK Government also intends to work with law enforcement to be able to better protect its citizens from cyber-attacks and to keep their personal and private information safe. Promoting security best practice when dealing with cyberspace in general on a day-to-day basis is another practical step the United Kingdom intends to follow;[141] regardless of whether a company or institution is big or small, best practice behaviours are essential to all. This is something that has already been mentioned earlier in this thesis, and it is one that in general is quite essential to keep networks and systems safe from cyber-attacks, and in this case especially, from human error. It is also essential to have a single incident management system, capable of registering cyber incidents, and able to analyse and discern the nature of all cyber-attack, so that a better and larger understanding of this threat is gained and readily accessible to all sectors who require it, leading to an effective information-sharing system. In this way, responses to cyber-attacks or the cyber defence itself can be finely tailored to each type of attack.[142]

The second objective is one of deterrence; focusing specifically on hostile foreign powers, in regard to the UK national strategy, there are a few points, such as reinforcing the application of international law within cyberspace as well as the promoting the voluntary agreement of non-binding norms of responsible state behaviour. The United Kingdom also believes that working with international partners and allies is essential to creating a credible deterrence, especially through the use of collective defence, something that NATO offers and beneficial advantage that the UK are eager to add to their deterrence arsenal. Information-sharing with international partners is also part of the United Kingdom's deterrence strategy; this works in a similar way to the first objective mentioned above, by exchanging information

[141] Cabinet Office and HM Government, NATIONAL CYBER SECURITY STRATEGY 2016-2021 § (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, 33-5.
[142] Ibid., 44-5.

and knowledge regarding cyber threats and how these threats have evolved or how they will evolve in the future, knowledge that is invaluable when dealing with new cyber threats. Attributing publicly "cyber identities" or actors who conduct cyber operations against the United Kingdom – when it is deemed in the UK's national interest – is another effective method of deterrence used by many states that this thesis will explore further on; this form of deterrence is akin to public shaming, denouncing someone, or in this case a state or actor, for their ill conduct against another, which in turn leads to an international bad reputation that may have political, social and economic consequences for said state or actor. The United Kingdom also intends to learn from other states and their cybersecurity policies and the effects they produce and use them to influence their own cybersecurity strategy, adding effective methods into the strategy while avoiding mistakes or less effective methods used by other states.[143] As mentioned above, the United Kingdom, like the United States focus on a more offensive based form of cybersecurity and defence; this applies to its deterrence as well. The UK therefore intends to build on this and allow offensive cyber capabilities to be made readily available to all branches of their Armed Forces, so that they may deploy them when they see fit, be it for deterrence or offensive operations, all within the confines of national and international law.[144]

The third and final objective is that of development, aiming to develop a fast-growing cybersecurity industry and cybersecurity skills within the United Kingdom, essentially dedicated to the acquisition and strengthening of tools and capabilities the UK needs to protect itself from any cyber threat or attack. To be more specific, the UK Government seeks to invest in private security companies so they are able to grow substantially quicker than they would alone, benefiting the state of the UK's cybersecurity as a whole. The government also intends

[143] Ibid., 48-50.
[144] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 15-6.

to recruit the best minds from all sectors of society, be it academia, the private sector, or from government itself, all to work together to more effectively spur innovation and new solutions in the world of cyber, providing training and mentoring to academics and using the private sector and other resources to make innovations into reality. This would be done through the establishment of two innovation centres that would drive the development of cutting-edge cyber products and technology, as well as the provision of testing facilities for (cyber) companies looking to test and develop their products, alongside a form of fast-tracking when it comes to the assessment of the next generation of cyber security tools and products, as well as services that may emerge, leading to more customer confidence and more investment in that sector; helping companies of all sizes scale-up and grow and granting them access to international markets coupled with a new initiatives programme would offer support to start-ups working in the realm of cyber, allowing them to get their first customers and spur on more investment opportunities, as well as the allocation of a proportion of the £165 million Defence and Cyber Innovation Fund that would support innovative procurement in defence and security. Still within this section, the UK Government believes that the UK's horizon scanning needs to be far more effective; horizon scanning is a method within futures studies that detects and assesses early on any emerging technologies or threats in a domain of choice, usually for policymakers. This will allow for a clearer anticipation and proofing against of any potential future threats and/or technologies, and can allow for a more cost effective decision-making strategy considering the vastly more tailored assessments will allow the UK Government – or any other government – the possibility focus on specific areas rather than a more generalized proofing of the country's systems and networks as well as its other defences. Therefore, the United Kingdom intends to implement more rigorous horizon scanning and have them integrated within every defence agency within the UK as well as cybersecurity and other technology policy development areas, capable of more finetuned assessments and analysis, as

well as with the capabilities to generate recommendations to inform present and future government policies; this will be done by identifying gaps in place to better create a more holistic approach to horizon scanning for cybersecurity, promoting better integration within behavioural science of the technological aspects of cyber security, and monitoring the cyber-criminal markets for any new tools and technology that could potentially end up in the hands of terrorist organizations or any hostile state. It is important to note that horizon scanning is subject to different types of variables, be it political, legislative, social, economic and environmental. This means that it must take into account these factors and any shift these tides may take, anticipating what may come due to such shifts. These shifts may and have had cybersecurity implications, meaning that careful decision making from policymakers is essential to guarantee a nation's cybersecurity and relevant cyber policies, in this case, those of the United Kingdom; informed and evidenced-based cyber-policymaking is therefore essential.[145]

The UK's National Security Strategy also outlines and lays the groundwork for the creation of the National Cyber Security Centre (NCSC). This organization is the central national body for cybersecurity at the national level, meaning it has a prominent role when it comes to coordinating sectorial cyber policies. It was launched in 2016, and is headquartered in Victoria, London and currently employs around one thousand (1000) employees and experts, a goal they set for 2021 that they were able to accomplish; it is composed of the Centre for Cyber Assessment (CCA), the Centre for the Protection of National Infrastructure (CPNI), the UK National Computer Emergency Response Team (CERT-UK), and the National Technical Authority for Information Assurance (CESG), which was the information assurance arm of the GCHQ. The NCSC works with ministries and government agencies and departments for the

[145] Cabinet Office and HM Government, NATIONAL CYBER SECURITY STRATEGY 2016-2021 § (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, 55-61.

implementation of cybersecurity programmes; it also works collaboratively with other law enforcement and defence sectors as well as the UK's intelligence and security agencies, and with international partners. The NCSC provides a single point of contact for small and medium enterprises (SMEs), along with larger organizations and the general public. The NCSC is able to have the fullness of situational awareness in the realm of cybersecurity due to its close collaboration with the GCHQ, permitting the former to draw on confidential security information, as well as support from high-level technical expertise; this includes industry and academic expertise. Through this expertise and situational awareness, the NCSC can understand cybersecurity, and therefore can distil this knowledge into practical guidance that is then made available to all, reducing the harm any potential cyber-attack or any other cybersecurity incident may cause on the wider UK. The NCSC also coordinates the actions of the Cyber Security Operations Centre (CSOC), which is the Ministry of Defence's centre for defence and response in case of cyber-attacks directed against the Ministry's infrastructures and systems, also securing public as well as private networks; in the event of a highly impacting cyber-attack the CSOC may receive backup from the United Kingdom's Armed Forces.[146]

As we have seen above, the United Kingdom focuses on an Active Cyber Defence, therefore, it relies on a variety of options when it comes to their cyber defence and security. This means it must not only be passive in its defence, such as responding to cyber-attacks, but also by actively engaging adversaries so as not to present an opening or vulnerability for a possible cyber-attack. Since the UK favours an offensive strategy to their cyber defence, they must have the capabilities to do so, and to carry out their cyber operations. These capabilities and operations are revealed in the UK Parliament's Intelligence and Security Committee's 2016–2017 Annual Report, and included are, but not limited to: the ability of retaliation in the event of a cyber-attack on the United Kingdom, the "*capability to deny, disrupt or degrade*

[146] Ibid., 37-8.

target communications or weapons systems (including shutting down the source of a [cyber-attack] or in preparation for more traditional military activities)"[147], and to have the capabilities to attack a wider range of systems and infrastructure which may extend to physical damage outside cyberspace, i.e. in the "real world"; these capabilities were developed already in 2014 by the United Kingdom's National Offensive Cyber Programme. When it comes to rules of engagement in regards to offensive cyber capabilities and deployment of cyber weapons, there are no clearly defined or internationally recognised regulations or frameworks; to that end, the United Kingdom has played a major role when it comes to seeking international agreements in this area, primarily through the biannual – previously annual – event known as the Global Conference on Cyberspace (GCCS) also known as "The London Process". This event was first held in the London in 2011, and has since been hosted in Budapest, Seoul, The Hague, and New Delhi, and is sponsored by the United Kingdom. In this conference, world governments, the private sector and civil society come together to support practical cooperation in cyberspace, promote the exchange of knowledge and expertise, enhance cyber capacity building and discuss norms for responsible behaviour within cyberspace. The importance of operating at an international level necessitates the cooperation between several states and other international partners. To that end the United Kingdom, along with Australia, Canada, New Zealand, and the United States of America cooperate with each in what is known as the Five Eyes (FVEY) Network, a close international intelligence partnership where these five members agree and commit to not spy on each other and to share detected intelligence signals. Following the same line of consistency, the United Kingdom is also part of the Nine Eyes Network – which consists of the same five members of FVEY along with Denmark, France, the Netherlands, and Norway – and the Fourteen Eyes Network (or SIGINT Seniors Europe) –

[147] Dominic Grieve, Intelligence and Security Committee of Parliament Annual Report 2016–2017 § (2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727949/ISC-Annual-Report-2016-17.pdf, 43.

which includes members of Nine Eyes along with Belgium, Germany, Italy, Spain and Sweden. Nine Eyes and Fourteen Eyes have a varying degree of intelligence sharing, with less access to shared information as the networks increase in number; this means that Nine Eyes sharing less than FVEY and Fourteen Eyes sharing even less than Nine Eyes. This intelligence sharing and international cooperation is essential for a cyber nation to gain an upper hand against potential adversaries, allowing for earlier detection and more effective horizon scanning, as well as potential access to new technologies in cyber that may better allow the United Kingdom to guard against potential new cyber threats; this in turn applies also to allies in this partnership, most of which are part of NATO, making the Alliance far stronger and interconnected when it comes to development of new capabilities and the proactive cyber defence of each member-state, and as a consequence, of the entire Alliance.[148]

4.3. France

As mentioned above, France, with a National Cyber Security Index of 84.42,[149] and like the United States and the United Kingdom, has opted for a more active form of cyber defence and security, which means, defence through active engagement against adversaries, deterrence through active offensive operations if you will. It is however important to note that unlike its Anglo-Saxon partners – whose cyber defence capabilities are concentrated within the intelligence community – the French have opted to separate their offensive missions and capabilities from their defensive missions and capabilities, stating that "*[b]y distinguishing the missions and resources dedicated to cyber protection, which are entrusted to the National Cybersecurity Agency of France (ANSSI), from those whose aims involve intelligence and offensive action, it facilitates the acceptance of State intervention in the security information*

[148] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 13-6.
[149] NCSI, "France," National Cyber Security Index, accessed September 3, 2022, https://ncsi.ega.ee/country/fr/.

systems, whether in public administration or the economic sphere."[150] To do this France has set the goal of a national system of cyber protection and defence, which, according to the French Government, would require the mobilization of relevant resources and the different skills and capabilities required from within the state itself but also from French society.

The French Strategic Review of Cyber Defence (*Revue Stratégique de Cyberdéfense*) states a few concerns when it comes to cyber deterrence and dissuasion; one of these is the lack of clarity regarding the modalities and systems that would be used for that dissuasion and in what manner these modalities and systems ought to be conducted. The difficulty in this regard stems from the fact that, as opposed to conventional and nuclear deterrence, cyber deterrence is not so black and white; it is a layered system, that is, one attack does not entail an automatic response from the affected party. While with nuclear deterrence an attack would entail a relatively simple and proportionate response, cyber-attacks will have a response depending on the gravity of the attack, the systems affected, and the type of attack conducted, in other words, there are a number of different factors that will end up influencing how cyber deterrence functions, so there is no guaranteed response or a proportionate response from the affected party, which in turn defeats the purpose of the concept of "deterrence", revealing its ineffectiveness, since the aggressor knows that a non-response or a non-proportionate response is a possibility. The second concern relates to how effective cyber, and cybersecurity is as a form of deterrence. In essence, it focuses on the destructive effects and consequences of cyber-attacks; unlike nuclear weapons, that are capable of near total destruction of entire cities or regions, cyber-attacks do not necessarily have those capabilities, albeit depending on the country conducting said cyber-attacks and the capabilities that country actually has. At most, cyber-attacks can gravely cripple a nation's critical infrastructure, leading to a variety of

[150] SGDSN, Strategic review of cyber defence § (2018), https://www.sgdsn.gouv.fr/files/files/Publications/revue-cyber-resume-in-english.pdf, 5.

effects, depending on the target; but mainly it can leave a country or part of it without electricity or without internet which in turn can lead to negative economic effects due to the increasingly digitalized nature of businesses, or it can lead to, for example, emergency services being unable to respond to any emergency that may arise after the cyber-attack. So, while cyber-attacks can have destructive effects, some of which irreparable, they are not comparable to the destructive nature of nuclear weapons, especially when damages caused by a cyber-attacks can be reversed in a small period of time, whereas damages caused by nuclear weapons are not so quickly reversed, and indeed may never be reversed, such is the finality of nuclear weapons, hence their dissuasive power, one that cyber does not possess, and may indeed never possess. Lastly, the third concern relates to the inability to monitor or limit the proliferation of ICTs used for offensive purposes; this inability/difficulty stems from the fact that cyber capabilities are essentially developed within cyberspace, not necessarily needing physical real-world places to do so. It is quite simple to monitor the proliferation of nuclear weapons due to it requiring large installations, great quantities of resources that can be detected and traced and relies on specific types of resources such as uranium. So, detecting and monitoring cyberspace and cyber capabilities can be an outright impossible, and therefore, impractical task. It is also very difficult to know whether these ICTs are being developed for offensive purposes or for defensive purposes, essentially rendering them non-malicious. Another factor that is not seen with nuclear arms is the fact that ICTs can be privately owned; nuclear weapons, unlike cyber capabilities, are not, and have never been, privately owned. This would mean that these non-state actors may not only act on their own accord when it comes to ICT proliferation, but it may indeed be impossible to enforce limitations on these non-state actors' proliferation efforts.[151]

[151] SGDSN, Revue stratégique de cyberdéfense § (2018), https://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf, 37-8; Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia,

There needs to be an outline of priorities when building a capable cybersecurity and defence initiative; one of the main priorities outlined is the strengthening of the nation's vital systems' resilience, which not only includes the State's, but also the country's critical infrastructure, so that it is able to withstand any potentially damaging cyber-attack directed at France. The State's most sensitive networks however must possess an uncompromising level of security; this would include for example submitting sensitive IT projects as soon as they are launched to ANSSI for opinion or optimising the use of the State's inter-ministerial network, making use of the security services it offers, which would make it possible for a more effective reaction in the event of a cyber-attack. The State's inter-ministerial network differentiates between offensive cyber capabilities, which includes offensive operations and information gathering – and defensive capabilities – such as asset protection. According to the French Strategic Review, this division allows for better military coordination when it comes to cyber defence, and also a faster reaction to a cyber-attack. This coordination is done by the "*Centre de coordination des crises cyber* (C4)", which brings together all relevant ministries concerned with defence and cybersecurity, allowing for a more appropriate response in the event of an attack, depending on the scope of such an attack. This network/agency works in cooperation with the French Cyber Defence Command (*Commandement de la cyberdéfense*, COMCYBER), which was established in May 2017, and is responsible for security and defence of military systems, including those of the Ministry of the Armed Forces, operations and infrastructures. COMCYBER is deployed in Paris and Rennes, and its duties also include coordinating the nation's cyber defence strategy, such as the contributions of national forces as well as those from international organizations – such as NATO – to the country's cyber defence policy in particular for the development and implementation of cooperation plans;

February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 17.

COMCYBER also exercises command of over 3600 cyber combatants and hopes to increase that number to 5200 by 2025. COMCYBER and its conduct is guided by a complete set of doctrinal corpus for defensive computer warfare (*la lutte informatique defensive*, LID), offensive computer warfare (*La lutte informatique offensive*, LIO), and cyber influence warfare (*La lutte informatique d'influence*, L2I); these doctrinal texts guarantee structured and consistent action and allows for a rapid mobilization of cyber resources.[152]

When it comes to safeguarding critical infrastructures, the Government outlines a few solutions, for example, increasing the security regulation requirements that are applicable to operators within the electronic communications and electricity supply sectors, as well as digital service companies, since these could gravely impact the nation and its ability to defend itself in the event of a cyber-attack. Taking it a step further, France wishes to transposition its Network and Information Security (NIS) Directive to protect a wider range of activities, such as essential services, gradually establishing a common set of proportionate rules on cybersecurity. At a European level, France seeks to have these rules adapted to each member-state, depending on their level of maturity in the area of cybersecurity. One point the French have outlined in the Strategic Review is the preservation of democratic institutions and way of life; as we will see further ahead, cyberspace can be greatly exploited to diminish a country's democratic institutions by lessening citizens' faith in said democratic institutions. This can be done directly, through manipulation of online voting systems, or indirectly, through misinformation campaigns online carried out by internet "trolls". The French Government seeks to combat these two aspects that threaten cyberspace through the "*pre-deployment of a*

[152] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 16-18; COMCYBER, ed., "Les Missions et La Chaîne de Commandement Du Commandement de La Cyberdéfense," Defense.gouv.fr, accessed November 3, 2022, https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber.

robust digital identity"[153] when it comes to online voting, and through the institution of an independent observatory that would be responsible for analysing the propagation of "fake news" and other misinformation campaigns while working in conjunction with digital operators to reduce these elements online as much as possible.[154] Touching on the private sector, the French Government has, within the action plan for small and medium enterprises (*Action Petites ou Moyennes Entreprises, Action PME*), promoted a system that allows companies to test their products and verify whether or not these products' cyber resilience is capable and strong enough, and in the event it is not, the system helps to improve that cyber resilience; this system costs a total of €4.5 million with half of these costs covered through subsidies.[155]

The French Government also wants to focus on exercising its digital sovereignty, allowing France to retain autonomy, allowing for it to appreciate, decide and take action within the digital space. France is particularly worried that, due to the digitalization of society as a whole, adversaries or cyber criminals in general may attempt to exploit this, infringing on the traditional elements of sovereignty. One of these elements is that of cloud computing; and how the cloud market is strongly dominated by a considerably small number of foreign companies, which, in the optic of the French Government, could potentially affect the nations digital sovereignty. Therefore, solutions have been presented by the Government, such as the establishment of a global policy for use of cloud computing by the State, which would be done by combining the use of the State's internal clouds and the use of cloud providers certified by the National Cybersecurity Agency of France, or ANSSI (*Agence nationale de la sécurité des systèmes d'information*); through the promotion of the development of cloud encryption

[153] SGDSN, Strategic review of cyber defence § (2018), https://www.sgdsn.gouv.fr/files/files/Publications/revue-cyber-resume-in-english.pdf, 8.
[154] Ibid., 6-8.
[155] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 19.

solutions such as homomorphic encryption techniques that allow the processing of encrypted data within the cloud; by supporting European strategic autonomy on the subject, both by investing in breakthrough technologies and by ensuring that fairness is restored between European players and their international competitors; the establishment of a global framework of trust so that businesses, communities and individuals can assess the risks associated with the use of cloud computing and its services; and finally, by developing the SecNumCloud certification for cloud providers, including at European level.[156]

Alongside this priority, the French Government states that "*operators essential to the functioning of [the French] economy and society, to the continuity of public services and to the preservation of [French] democratic life, must also be better protected.*"[157] The promotion of a culture of digital security in society is also one of the priorities of the French Government. As we have mentioned in the beginning of this thesis, humans and human error are frequently the reason why a system is breached, many times due to ignorance of said person of cybersecurity. Therefore, a well-informed populace with common knowledge of the risks regarding cyberspace and information and computer use is essential to guarantee the integrity of potentially vital infrastructure systems in any given nation. The Government seek to achieve this through a pedagogical approach in order to increase its impact and fully engage everyone's interest in digital issues. According to the French Government, this could be done through digital education in primary and secondary schools, making it a requirement for a student to achieve the lower secondary school certificate, and should be integrated into all upper secondary course curricula. Teachers that would teach this should have regular training by the Ministry of Education in collaboration with ANSSI, allowing these teachers to remain up to date on new information regarding cyberspace that they would need to pass down to students,

[156] SGDSN, Strategic review of cyber defence § (2018), https://www.sgdsn.gouv.fr/files/files/Publications/revue-cyber-resume-in-english.pdf, 10-1.
[157] Ibid., 3.

alerting them of new threats that may arise as time goes by and technology evolves, so that they too can remain up to date regarding cybersecurity and good practice behaviour in cyberspace. When it comes to those that are no longer children or young adults, the French Government believes that within higher education courses, where there is no specialization in digital security, a form of cybersecurity a training program may be integrated into a course, such as law or economics, so that these students are aware of the dangers within cyberspace. These training programmes could also be extended to be included into businesses' yearly seminars and team building exercises, which would in turn support the digital transformations of said businesses.[158]

The French Government seeks also to reinforce its strategic thinking with regards to cyberspace as a whole and focus on creating diplomatic relations within this area, via either international organizations such as the European Union or NATO, smaller accord groups such as the aforementioned Nine Eyes and Fourteen Eyes Networks, or via bilateral diplomatic agreements, all in favour of a collective and controlled governance of cyberspace. With regards to NATO, the Strategic Review states the need and importance of strengthening NATO's cyber defence capabilities, primarily through NATO's aforementioned Cyber Defence Pledge – agreed on in the 2016 Summit – which would allow France to be better integrated in NATO's operations and missions.[159] The Government wishes for France to have a willingness to build a strategic stability based on a peaceful and prosperous cyberspace where fundamental freedoms and right are respected. France also differs with the examples that we have so far examined, insofar as France seems to have European concern for cyberspace rather than a solely national concern, stating that the Government's aim for cyberspace is to "*help bring*

[158] Ibid., 13-4.
[159] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 19.

about a digital Europe that is safe and reliable";[160] this is however not a surprise given President Emmanuel Macron's Europhilic views.

The French Strategic Review has separated and sorted its cyber defence missions into six categories, these being: prevention, anticipation, protection, detection, attribution, and reaction. These cyber defence missions are then inserted into one of the following four operational chains, these being: protection, military action, intelligence, and judicial investigation. The "protection" chain is under the responsibility of the French Prime Minister but run by the General Secretariat for Defence and National Security, or SGDSN (*Secrétariat Général de la Défense et de la Sécurité Nationale*), working in collaboration with ANSSI, with the responsibility for operations management falling under the purview of the ANSSI's Director General; the commander of cyber defence is also delegated from ANSSI and is responsible for operations carried out within the wider scope of the Ministry of the Armed Forces. The purpose of this "protection" chain is to ensure that national security is maintained in the event of a cyber-attack, or any other potential cyber threats. The "military action" chain falls under the purview of the President of the French Republic, who is in turn the Chief of the Armed Forces; this chain can use active cyber warfare capabilities and allows for national defence operations to be carried out. The "intelligence" chain falls under the French Government's purview, covering all actions that are undertaken for intelligence purposes, such finding the culprit of a cyber-attack and publicly attributing that attack to said culprit; this chain also implements offensive cyber capabilities. Regarding the "judicial investigation" chain, it covers essentially the actions of the French police and its national gendarmerie, as well as its justice services, following an investigative framework.[161]

[160] SGDSN, Strategic review of cyber defence § (2018), https://www.sgdsn.gouv.fr/files/files/Publications/revue-cyber-resume-in-english.pdf, 3.
[161] Ibid., 5-6.

4.4. Germany

As mentioned in the beginning of this section, the United States, United Kingdom, and France have a more proactive approach when it comes to their cyber defence and security. Now we will take a look at the first example of a country that is less so and is more defensive and reaction-based when dealing with their cyber defence. Germany – with a National Cyber Security Index of 90.91[162] – is one of the countries that incorporates the Fourteen Eyes Network and the Group of Governmental Experts (GGE) – a United Nations group focused on responsible State behaviour within cyberspace.[163] In Germany, cyber defence is entrusted to the German Armed Forces, or *Bundeswehr*; abiding by national and international legislation that regulates the activities of the *Bundeswehr*, the act of managing German cyber defence is done by the German Ministry of Defence. Germany's first approach towards dealing with cybersecurity officially began in 2011 when they released their first Cyber Security Strategy, succeeding 2005's National Plan for Information Infrastructure Protection, when the German National Cyber Defence/Response Centre (Cyber-Abwehrzentrum / Cyber-AZ) was created under the command of the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* / BSI); according to the official website: "*the organisations involved in the Cyber-AZ include the Federal Office of Civil Protection and Disaster Assistance (BBK), the Military Counterintelligence Service (BAMAD), the Federal Office for Information Security (BSI), the Federal Office for the Protection of the Constitution (BfV), the Federal Criminal Police Office (BKA), the Federal Intelligence Service (BND), the Federal Police Headquarters (BPOLP), and the Cyber and Information Domain Service (KdoCIR) as core authorities, along with and the Customs Investigation Bureau (ZKA) and the Federal Financial*

[162] NCSI, "Germany," National Cyber Security Index, accessed September 3, 2022, https://ncsi.ega.ee/country/de/.
[163] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 22.

Supervisory Authority (BaFin) as associated offices"[164]. The world of cyber is a complex one, and therefore it requires rapid response when it comes to defence, responses that must see beyond lines of jurisdiction that separate the responsibilities of different security authorities, so as to offer a more effective response, prevention and defence. So, to solve this issue, the Cyber-AZ adopted an inter-ministerial approach to facilitate the constant exchange of information among all the federal authorities with security responsibilities, be it on a federal (*Bundes*) level, or a local (*Länder*) level. This merges all warnings of potential cyber-attacks and allows for a coordinated response that is in line with national and international legislation. Throughout the years the Cyber-AZ has evolved from a simple information hub into a cooperation network, and, according to the official Cyber-AZ website[165], this has developed a strong bond between all those involved, resulting in a very effective team that works well in innovation as well as defending against cyber-attacks. This positive outcome within Cyber-AZ allowed for, in 2016, the possibility of carrying out offensive cyber operations as retaliation for cyber-attacks. The particularity of this is that Germany has a more passive and defensive approach as opposed to the more active and aggressive defence posture of the United States and the United Kingdom, yet they consider the possibility of carrying out offensive cyber operations, albeit as retaliation only. The 2016 Cyber Security Strategy also states that the Military Counterintelligence Service (*Militärische Abschirmdienst*, MAD) is also responsible for responding to malicious occurrences within cyberspace, to help to reach the highest levels of operational readiness; however, due to constitutional checks imposed by the German *Grúndgesetz*, or constitution, *Bundeswehr* contributions are limited. There is a constitutional separation in Germany between which body handles cybersecurity and which body deals with

[164] Bundesregierung, ed., "The National Cyber Response Centre," Federal Office for Information Security, August 2, 2022, https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum.html.
[165] Ibid.

cyber defence; due to this constitutional separation there is a nexus between *Bundeswehr* cyber defence capabilities and response capabilities within the framework of cybersecurity, as stated in the 2016 National Strategy and the 2016 German White Paper (on German Security Policy and the Future of the Bundeswehr)[166], although they are manged separately.[167]

Since the implementation of the 2016 European Directive on Network and Information Security (NIS Directive) – an EU-wide cybersecurity legislation that endeavours to enhance cybersecurity across the European Union through cross-border collaboration, increasing and/or improvement of national cyber capabilities, and national supervision of critical sectors, much of it done within the NIS Cooperation Group[168] – the BSI has been in operational command of cyber defence, doing so through the monitorization of federal government networks, investigating security accidents, and activating necessary defensive countermeasures. As mentioned before, the *Bundeswehr* has constitutional limits that keep it from collaborating with the BSI due to the nature of BSI operations, which are not considered "proper" operations, unlike operations carried out in response to a cyber-attack, that, due to its size, requires the deployment of the Armed Forces. The *Bundeswehr* also suffers from another particularity: the Armed Forces requires approval from the *Bundestag* to carry out operations within German territory, and cyber defence is not exempt from this due to cyber defence being considered a military operation within German territory, and, as we have seen earlier, the world of cyber moves very fast, too quickly to wait for parliamentary approval, which would hinder any effective response towards the attack; however, if the cyber defence operation is within a

[166] Ministry of Defence and Bundesregierung, WHITE PAPER 2016 ON GERMAN SECURITY POLICY AND THE FUTURE OF THE BUNDESWEHR § (2016), https://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf, 38.
[167] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 20-1.
[168] ENISA, ed., "NIS Directive," European Union Agency for Cybersecurity, October 13, 2022, https://www.enisa.europa.eu/topics/nis-directive.

cooperative framework, the initial approval by the *Bundestag* of that whole operation is enough to sanction it, resulting in a sort of workaround, allowing for a more effective cyber defence response.[169]

The Cyber and Information Space Command or Cyber and Information Domain Service (*Kommando Cyber- und Informationsraum*, CIR) is also another service of the *Bundeswehr* that was set up in the 2016 German White Paper, aiming for full operations and 14,000 personnel units by 2021; today the CIR consists of 14,500 personnel, 28 departments, and it is located in 25 different sites. Its core task is to protect and operate the *Bundeswehr*'s IT infrastructure – in this case its IT systems and services – and through its Communication and Information Systems Services Centre it exercises command and control of servicemen in six German CIS (Communication and Information Systems) support battalions as well as one NATO Signal Battalion. The CIR also provides training for their servicemen and recruits at their *Bundeswehr* Communication and Information Systems School and has also been the leading authority in "*innovation, software development and integration, certification of IT services and cross-service simulations in the armed forces*"[170].

Germany highlights the need to operate within a regulated framework, in all aspects of military or civil governance, however, the reality, within cybersecurity in Germany, is that active defence operations are not currently explicitly regulated, which limits Germany's actions and has led to debating on a national level regarding this issue, especially when it comes to the issue of "hack-backs" in response to cyber-attacks. Another area the German Government has focused on is in working with the private sector to better guarantee the country has adequate and state-of-the-art technology. This was done by setting up the Agency for Innovation in

[169] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 21.
[170] Bundeswehr, "The Cyber and Information Domain Service," Bundeswehr, accessed November 15, 2022, https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service.

Cybersecurity whose aim is to "*promote the development of innovative solutions in the field of cybersecurity. It also aims to help Germany to increase its own technological sovereignty in cybersecurity*"[171], as well as to sign contracts for research projects; the agency has received, and will continue to receive until 2023, over €350 million in funding.[172]

4.5. Spain

Regarding cybersecurity, Spain is one of the countries that has, at an early age, taken cyber threats seriously. As far back as 2008, Spain – with a National Cyber Security Index of 88.31[173] – had already created not one, but two centres focused on rapid response in the event of cyber-attacks, these being the Spanish National Cybersecurity Institute (*Instituto Nacional de Ciberseguridad*), or INCIBE-CERT, and the National Cryptologic Centre (*Centro Criptológico Nacional*), or CCN-CERT. The INCIBE-CERT is focused on responding to cyber-attacks directed at civilian infrastructure and assets, such as businesses or private citizens, while the CCN-CERT's task is to respond to cyber-attacks aimed at governmental institutions and networks. Within the Spanish Military lies the Cyber Defence Joint Command, or *Mando Conjunto de Ciberdefensa* (MCCD), as well as its own Computer Emergency Response Team (ESP-DEF-CERT), established in 2013, which is responsible for enacting operations regarding the cyber defence of ICT systems and infrastructures linked to the Spanish

[171] Bundesdruckerei, "Tasks of Germany's Cybersecurity Institutions," Bundesdruckerei, accessed November 16, 2022, https://www.bundesdruckerei.de/en/innovation-hub/name-cybersecurity#:~:text=In%202018%2C%20the%20German%20government,in%20the%20field%20of%20cyber security.
[172] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 21-2.
[173] NCSI, "Spain," National Cyber Security Index, accessed September 3, 2022, https://ncsi.ega.ee/country/es/.

defence apparatus, including the cyber integrity of said systems; in the event of a cyber-attack, the MCCD contributes to the appropriate response with the relevant CERTs through its ESP-DEF-CERT. A detailed outline of the several institutions and branches involved in Spanish cybersecurity, as well as their relationships and interoperability, can be seen in *Figure 5*[174]. Due to the sheer size of the cyber domain the MCCD follows a series of operational guidelines to help them prioritize the many cyber assets that require protection, using those guidelines to define which assets would need protection depending on the scale and magnitude of a potential cyber-attack. The MCCD is subordinated to the Spanish Defence Staff, and so therefore, these cyber operations can be integrated into the command structure of multinational institutions such as NATO, as well as other organizations like the European Union and the United Nations; however, offensive cyber operations are unable to be carried out if there is no ongoing declared armed conflict, which is a stark contrast to other countries that integrate NATO such as the United States and the United Kingdom, which do not require declared armed conflicts to carry out offensive cyber operations.[175]

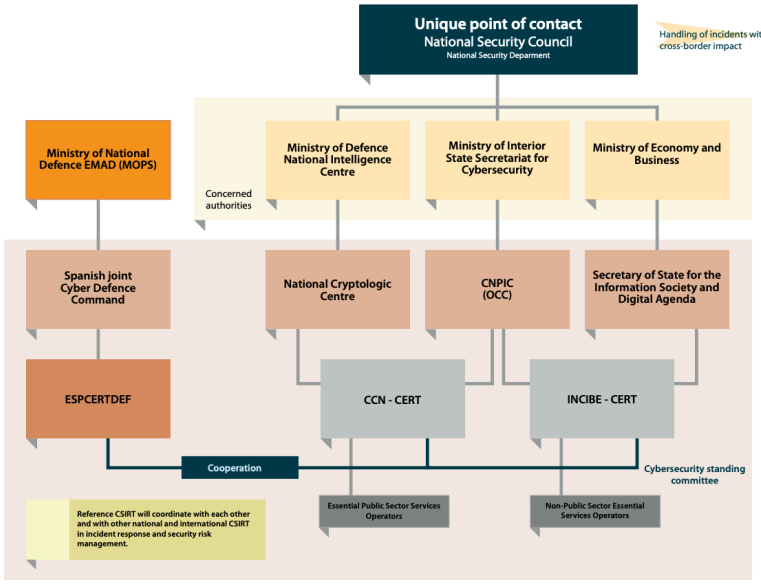

Figure 5: Actors in Spanish National Cybersecurity.

Despite all this, Spain remains one of the most affected countries in Europe where its cyberspace has fallen victim to frequent cyber-attacks over the years; and while some of these

[174] Ministerio de Defensa, ed., *Spanish Approach to Cybersecurity*, June 2019, https://www.ccn.cni.es/index.php/en/docman/documentos-publicos/23-decalogue-spanish-approach-to-cybersecurity-2018/file, 13.
[175] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 23-4.

cyber-attacks were directed on civilian infrastructure and sectors, other attacks were consistent of cyberespionage – which, as we shall see further ahead, can have some quite injurious effects, be it on the private or public sector – which had some quite severe consequences, specifically regarding sensitive information. The most prominent case is the prolonged cyber-attack on the Spanish Ministry of Defence in 2019, where a virus introduced through email gained access to an intranet network of over 50,000 users in search of information on sensitive military technology.[176] Due to this, and an overall increase in cyber threats, a year later in 2020, the Spanish Royal Decree nº 521/2020 was issued, which focused on the organization of the Spanish Armed Forces, emphasising the need to have more adequately trained as well as technologically advanced staff when it comes to digital transformation within the Armed Forces, and that it's defence systems along with other structures follow suit. Due to the ongoing SARS-CoV-2 pandemic that started in 2019, the 2017 National Security Strategy was updated in 2021 to take prolonged pandemics into account and how that can affect the cyber domain. This is due to the fact that during this pandemic many people were instructed to remain at home, forcing them, as well as businesses, to adopt new ways to engage with each other. For example, many people began working from home, using new software and depending greatly on the use of the internet to do so; this meant new potential vulnerabilities and cyber threats which needed to be taken into account by the relevant authorities. This meant upgrading systems and modifying strategies to take this new reality into account, and to be better prepared in the event of another pandemic at this scale.[177] This decision by the Spanish Government follows European Union's Security Union Strategy, with regards to force majeure events such as pandemics and EU-level coordination when it comes to non-traditional threats, of which

[176] Reuters, "Computer Virus Infects Spain's Defence Ministry: Report," *WION*, March 26, 2019, https://www.wionews.com/world/computer-virus-infects-spains-defence-ministry-report-205782.
[177] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 23-4.

cyber threats are therein included; the EU Security Union Strategy states that: "*(...) the Commission will explore a possible EU-level coordination mechanism for police forces in case of force majeure events such as pandemics. The pandemic has also proven that Digital Community Policing, accompanied by legal frameworks to facilitate online policing, will be fundamental in tackling crime and terrorism*"[178], and by extent cyber-attacks conducted by foreign powers or other third-party organizations.

Following on from the last point, Spain is acutely aware of the need for a deeper international cooperation when it comes to cybersecurity and defence. As we have just mentioned, Spain has taken most of its cyber defence policies form the EU Security Union Strategy, paying particular attention to the need for awareness within cyberspace, both from its officials and its citizens. With regards to operators, be they civilian or military, Spain has focused greatly on providing specialized training to said operators, doing so through its aforementioned National Cryptologic Centre, as well as through dedicated partnerships between its INCIBE and the Ministry of Defence; these agreements also seek to train young people to be more aware in the cyber domain, further guaranteeing Spanish national cybersecurity. Spain has also lead projects, as well as other research centres around the world, within the European Defence Industrial Development Programme (EDIDP) and the European Cyber Situational Awareness Platform (ECYSAP), allowing for a clearer picture regarding specific cyber threats that can target defence systems of any country, which in turn allows for the relevant armed forces to respond with greater efficiency and speed to said cyber threats.[179]

[178] European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy § (2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN, 23.
[179] Ester Sabatino and Alessandro Marrone, "Cyber Defence in NATO Countries: Comparing Models," Academia, February 2021, https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models, 25.

4.6. Portugal

When it comes to Portugal it must be understood that, regarding defence, as a whole, Portugal, with a National Cyber Security Index of 89.61,[180] is relatively small and limited. As we mentioned at the beginning of this chapter, some nations suffer from a lack or deficiency of capabilities, or outdated capabilities, and talent that may hinder their ability to guarantee a nation's cyber defence and security, and we can examine Portugal as such an example, where it relies more so on international capabilities and organizations – such as NATO – to guarantee its defence. This is not to say however that Portugal is completely irrelevant or inept in dealing with its cybersecurity and defence; quite the contrary in fact, it is very well aware of the dangers of cyberspace, and by extension, malicious cyber actors, pose to the country, and therefore takes the necessary and diligent steps to guarantee its cybersecurity, as we shall see.

Like the countries we've seen in this chapter already Portugal also has a "cybersecurity strategy", as well as institutions and entities that handle the nation's cybersecurity and defence. It is, however, important to note that Portugal's strategy focuses more broadly on "cyberspace security", which includes both cybersecurity and cyber defence[181]. The national cybersecurity authority in Portugal is the Portuguese National Cybersecurity Centre, or "*Centro Nacional de Cibersegurança*" (CNCS), and the National Computer Security Incident Response Team is CERT.PT which integrates the Portuguese CNCS. Regarding the Portuguese national cybersecurity strategy, Portugal first elaborated one in 2015, a strategy that was then revised in 2019 to the current strategy, one that encompasses 2019 all the way to 2023, foreseeing regular checks and eventual updates where the need may arise.[182] The cybersecurity strategy

[180] NCSI, "Portugal," National Cyber Security Index, accessed September 3, 2022, https://ncsi.ega.ee/country/pt/.
[181] António Miguel Neves Almeida and António Gameiro Marques, Interview: Rear-Admiral António Gameiro Marques, personal, January 23, 2023. Refer to Appendix II, p. 175.
[182] Governo de Portugal, ed., "Estratégia Nacional de Segurança Do Ciberespaço," Portugal Digital, June 20, 2022, https://portugaldigital.gov.pt/acelerar-a-transicao-digital-em-portugal/conhecer-as-estrategias-para-a-transicao-digital/estrategia-nacional-de-seguranca-do-ciberespaco/.

outlines how in 2015, when the first strategy was first approved, the technological emergence had impacted the world, as well as Portugal, and how we all were growing evermore dependent of ICTs. This meant an increase in vulnerabilities within these new ICT systems (as can be seen in *Figure 6*[183]), which in turn meant an increased opportunity for those wishing to exploit and compromise said ICTs for personal, or even political gain. We saw examples of this in 2022, when Portugal suffered not one, but two cyber-attacks – with the severity of the second attack surpassing that of the first one[184] – within a relatively short period of time, which resulted in hundreds of secret and confidential NATO documents being stolen and put for sale on the dark web.[185] So therefore, the cybersecurity strategy would need to be able to keep up with this constant evolution of the cyber-scape.

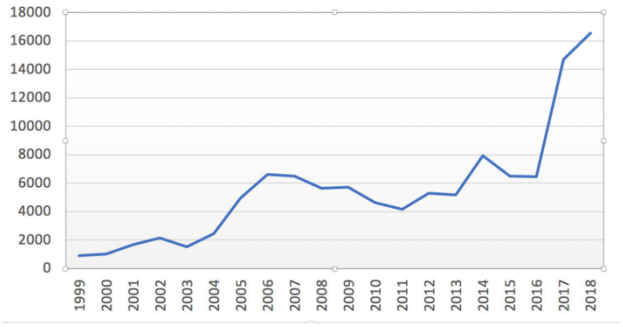

Figure 6: Number of vulnerabilities published per year in Portugal.

The 2019-2023 Portuguese Cybersecurity Strategy is founded on three principles, these being: the Subsidiarity, Complementarity, and Proportionality principles. The Subsidiarity Principle states that since most of what makes up cyberspace is owned by entities of the private sector, then responsibility of protection falls primarily on these entities, that it begins with the individual and ends with the State, stating that "*Considering that much of the technological infrastructure that makes up the cyberspace is owned by private sector entities, it is their primary responsibility to protect it. This responsibility begins in the individual himself, through the responsible way by which he uses cyberspace, and ends with the State, as the guardian of*

[183] CNCS, "Additional Recommendations," essay, in *National Cybersecurity Framework* (CNCS, 2020), 144, https://www.cncs.gov.pt/docs/qnrcs-web-eng.pdf.
[184] Natasha Donn, "Armed Forces Centre for Cyber Defence Suffers New Attack," *Portugal Resident*, October 2, 2022, https://www.portugalresident.com/armed-forces-centre-for-cyber-defence-suffers-new-attack/.
[185] Natasha Donn, "Hundreds of NATO Documents Sent to Portugal Discovered for Sale on Dark Web," *Portugal Resident*, September 8, 2022, https://www.portugalresident.com/hundreds-of-nato-documents-sent-to-portugal-discovered-for-sale-on-dark-web/.

sovereignty and the constitutional principles."[186] This principle prioritises individual responsibility and good conduct when using ICT equipment before relying on the State for help. This calls back to the beginning of this thesis, where we discussed how many times it is through the irresponsible use of the internet or other ICT tools that malware is able to breach into a system, or in this case, personal computers. The Complementarity Principle states that, since cyber-attacks and other incidents can propagate throughout all types of cyber actors, cybersecurity is a shared responsibility between all these actors, whether they are private or public actors, and whether they are collective or individual actors. This means that an inclusive, interdependent, integrative and comprehensive approach to cybersecurity must be adopted to minimise the effects of such potential cyber-attacks and maximise digital protection and resilience. Regarding the Proportionality Principle, it simply states that resources and cyber capabilities should be proportionally allocated to the necessary sectors according to potential risks identified and according to "action lines" defined and outlined in the cybersecurity strategy.[187]

The cybersecurity strategy sets out the following three strategic objectives: Maximize Resilience, which essentially focuses on strengthening cyber capabilities as well as promoting more ample networking to combat any threat may disrupt or compromise national networks; Promote Innovation, as the name suggests, it implies that the State focusses on promoting national innovation for economic, social and cultural development, as well as innovating cyber capabilities and tools; and Generate and Guarantee Resources, which aims at obtaining adequately allocating resources to increase Portugal's national cybersecurity capabilities.[188]

[186] Portuguese Republic, "ANNEX - National Strategy for Cyberspace Security 2019-2023," in *Portuguese Official Journal*, vol. 108 (Imprensa Nacional, 2019), 2889.
[187] Ibid.
[188] Ibid., 2890.

Following these three strategic objectives, the strategy presents six intervention "axes" as means to achieve said three strategic objectives. The first axis is "Cyberspace Security Structure", and it sets out several goals, beginning with the consolidation and reinforcement of the Superior Council for Cyberspace Security to act as a specific consultative body for the Portuguese Prime Minister. It also states the need to strengthen the CNCS as the Portuguese national cybersecurity authority, making it the single point of contact for any and all national and international cybersecurity cooperation purposes. Following this it seeks to strengthen its national cyber defence capacity so as to maximise the resilience of the Portuguese Armed Forces when dealing with cyber-attacks or other significant incidents, highlighting the use of offensive cyber capabilities as a response to said cyber-attacks. It also looks into the need to deepen the use of cyber defence capabilities for both national and international cybersecurity by "*developing and consolidating an information sharing system at various decision-making levels and thresholds;*"[189] this means that there needs to be greater coordination between the relevant entities that deal with cybersecurity and defence that make up the Internal Security System as well as relevant sectors, such as electronic communications and essential services. Since cybersecurity and defence involves a certain level of intelligence, this axis foresees the need to improve the Security Intelligence Service and the Strategic Defence Intelligence Service; the former has the exclusive responsibility to gather intelligence that may prevent sabotage, terrorism, espionage, and other disruptive and potentially destructive incidents, and the latter is solely responsible for gathering intelligence that contributes to the safeguarding of national interests, independence and external security of the Portuguese State. Finally, developing "*[cyber-diplomacy] as the discipline of the State's external action aimed at promoting, inter alia, the application of the existing international law to cyberspace in order to ensure its stability, the transparent and shared governance of its universal use and the*

[189] Ibid., 2891.

efficient creation of normative capacities,"[190] and most especially when it comes to the Community of Portuguese-Speaking Countries, or CPLP (*Comunidade dos Países de Língua Portuguesa*).[191]

The second axis refers to "Prevention, Education, and Awareness Raising", and when dealing with prevention it states that it is crucial to develop the ability to obtain knowledge on indicators that may be linked with potential and ongoing threats in an automated and systematic way, which would allow the entirety of the Portuguese national cybersecurity ecosystem to have ample knowledge to produce threat anticipation which in turn leads to a more effective cyber defence and security. This means effective collection of information and intelligence, knowing the threat agents as well as their intentions and capabilities, anticipating threat emergence and evolution to be able to better adapt to said threats. This is where education comes in: it means creating more resilient citizens through the development of digital skills, most notably through the National Digital Skills Initiative e.2030, and through awareness raising so that there may be a safer and more responsible use of ICTs, especially with younger and elderly generations; something that can be done also through school syllabi, regular training seminars in the workplace, or through training programs, especially when it comes to decision makers, public managers, and operators of critical infrastructures. This is something we have seen in other cybersecurity strategies, most notably in the French strategy, and something that is key to a complete and wide-ranging approach to cybersecurity. The Portuguese strategy takes it a step further and actively looks to identify young people with potential for cybersecurity to have them integrated into the professional context, adding to the overall increase in the number of specialists. Another, quite important, point referred in this strategy is the need to conduct regular exercises, allowing teams to train their abilities and

[190] Ibid.
[191] Ibid., 2890-1.

increase the overall preparedness and maturity the nation has in the event of a real cyber-attack; this, of course, includes participation in international exercises organized international organizations, such as NATO or the European Union. As well as exercises, Portugal seeks to take advantage of training programs and initiatives conducted by NATO and the EU, as well as building teaching structures used by said organizations in Portugal, a prime example of this being the NCI Academy, built in Oeiras. This Academy provides training services to NATO – and to the NCIA itself – and nations, but it aims to train not only military personnel, but also private citizens who may seek to enrol in the Academy. The Academy also has a legacy when it comes to CIS and C4ISR education and training and it offers "*Individual Training in the field of C4ISR and Cyber, on site at our new Academy facility in Oeiras or in our other locations, online or on-the-job; […] Collective Training and Exercise services, including support for the NATO Education Training Exercises & Evaluation (ETEE) software suite; […] Learning Innovation and Development services, to assist NATO and Nations in modernizing the methods and infrastructure related to training delivery.*"[192] Finally, the strategy seeks to promote specific awareness programs within both public and private institutions by not only training good conduct and responsible behaviour, but also by sharing specialized information on threat agents and methods to as well as sensitizing said institutions to potential vulnerabilities that could affect them.[193]

Moving on to the third axis, entitled "Cyberspace Protection"; cyberspace, and therefore security in cyberspace, is essential to a guaranteeing not only national security but also to guarantee national sovereignty, much like maintaining a security presence on land, air and sea. Therefore, to do this, the third axis seeks to do the following: to identify critical

[192] NCI Agency, ed., "NCI Agency: About the NCI Academy," NCI Agency | About the NCI Academy, accessed January 12, 2023, https://www.ncia.nato.int/what-we-do/nci-academy/about-the-nci-academy.html.
[193] Portuguese Republic, "ANNEX - National Strategy for Cyberspace Security 2019-2023," in *Portuguese Official Journal*, vol. 108 (Imprensa Nacional, 2019), 2891-2.

information infrastructure and reinforce knowledge on said infrastructures, while following changes in the nations legal framework concerning cyberspace; promoting the development of cyber capabilities and focusing on maturing national entities to prevent, detect, respond and recover from cyber-attacks, as well as promoting sectoral cooperation nationwide – public or private – to more effectively guarantee cyberspace security; applying incentives that would enable the "*development of national and international cyberspace security management frameworks and their adoption by national authorities with responsibilities for critical infrastructures and essential services*"[194]; and finally, to maximize the security and defence of the information networks and systems used by the Portuguese Armed Forces and the rest of its National Defence, while maintaining operational capabilities, as well as a presence, in cyberspace, specifically, through a defensive approach with regards to its cyber defence. As mentioned in this axis, infrastructure is an important aspect that must be given particular attention when it comes to its protection, especially critical infrastructure in a more general term.[195] While the Portuguese cyberspace strategy only refers to "critical information infrastructure", it should be noted that critical infrastructure in general has been widely talked and written about in Portugal, and, in an increasingly evolving and interconnected society, new elements have become recognizable as part of critical infrastructure. The Portuguese strategy, which was elaborated in 2019, will be phased out this year (2023), and a new strategy is expected to take its place, taking into account the current factors of cyberspace that have developed since 2019, one of these likely being critical infrastructure and not limited to critical information infrastructure, something the European Union itself has also explored and expanded on, going so far as to consider essential services as part of critical infrastructures; this would include health services, tax authority, social security, among others, essentially

[194] Ibid., 2892.
[195] Ibid.

meaning that critical infrastructure, today, is no longer limited to physical infrastructure, but virtual and/or non-tangible assets.[196]

The fourth axis focuses more on threat response, the ability of the Portuguese state to respond accordingly to attacks. To guarantee cyberspace security the strategy explains the need for a more proactive presence within cyberspace, to prevent and hinder possible attacks; likewise, the ability to carry out military operations within cyberspace is imperative to ensuring Portugal's freedom of action within cyberspace. As mentioned above, Portugal has a defensive approach to its cybersecurity, leaving its threat and attack response to its cyber defence element. To do this the strategy intends to enhance said threat response capabilities by reinforcing cooperation between existing cyber incident response teams and through the further creation of new cyber response teams in all public and private bodies. Also relating to public and private cooperation, the strategy refers to how the Armed Forces', Security Forces and Services', and other public and private entities' capabilities must be adapted for crisis management purposes, allowing for a more integrated approach when dealing with the risks and threats in cyberspace; as well as, in a collaborative manner, sharing knowledge on security threats between the relevant public entities and private entities that would allow for greater threat awareness, a more proactive attitude to said threats, and a clearer prevision of the impacts those threats may cause. Knowledge sharing has also put into question within this strategy the possibility of updating existing legal framework concerning data retention, and more importantly, data collection, such as the seizure of emails other similar forms of electronic communication. With that potential update to the legal framework in question the strategy also foresees the need to revise legislation concerning cyber, especially when it comes to

[196] António Miguel Neves Almeida and Paulo Viegas Nunes, Interview: Brigadier General Paulo Viegas Nunes, personal, January 13, 2023. Refer to Appendix I, p. 152-3.

institutional cooperation with the equivalent international entities.[197] It is important to note that, during our interview, regarding the element of legislation, Rear-Admiral António Gameiro Marques, the Director of the Portuguese National Office of Security (*Gabinete Nacional de Segurança*), believes that the current legislative structure is incapable of keeping up with the rapid evolution of cyberspace and cyber capabilities, and thus, incapable of responding adequately to new cyber threats. In his opinion, legislation regarding cyber should take a more generic and outlining approach, leaving any specific elements to the relevant authorities, through technical norms, allowing for a more dynamic and streamlined response when dealing with evolving elements and threats.[198] Regarding this approach, the coordinator of the National Cybersecurity Centre Lino Santos acknowledged the potential need to expedite certain legislative cycles, but emphasised that legislation should not be drawn up in a "vacuum", rather, legislation exists as a response to a problem, and so it should continue to be, amended where it needs to be.[199]

The fifth and penultimate axis focuses on innovation and R&D (Research and Development); where the aim essentially is to not only to focus on R&D nationally, but also internationally. This means promoting scientific R&D in the various fields concerning cyberspace, including cyberspace and cyber defence, and the development of systems and services that are "secure by default" and "secure by design"; it also means promoting foreign investment in cyberspace security and enhancing ongoing cooperative efforts within international organizations, such the European Union or NATO, in which Portugal is an integrating member. Portugal focuses on pooling and sharing information, as well as smart defence with the EU and NATO respectively, while engaging in multinational collaborations

[197] Portuguese Republic, "ANNEX - National Strategy for Cyberspace Security 2019-2023," in *Portuguese Official Journal*, vol. 108 (Imprensa Nacional, 2019), 2893.
[198] António Miguel Neves Almeida and António Gameiro Marques, Interview: Rear-Admiral António Gameiro Marques, personal, January 23, 2023. Refer to Appendix II, p. 182.
[199] António Miguel Neves Almeida and Lino Santos, Interview: Coordinator Lino Santos, personal, February 13, 2023. Refer to Appendix III, p. 204.

with universities, research centres, and industry, allowing Portugal to develop new solutions that can have both a military and civil use, as well as participating in technical committees – both national and international – to "*implement internationally accepted technical standards and specifications applicable to the security of network and information systems*"[200]. The strategy elaborates on the need to train public officials, specifically, this would be done through the Strategy for Digital Transformation in Public Administration (*Estratégia para a Transformação Digital na Administração Pública*) and the Digital Development Strategy National Digital Skills Initiative e.2030 (*Iniciativa Nacional Competências Digitais* e.2030 – INCoDe.2030). Both the Coordinator of the National Cybersecurity Centre Engineer Lino Santos as well as Brigadier General Paulo Viegas Nunes also refer to a training program led by the National Cybersecurity Centre with similar objectives called C-Academy. The Coordinator Lino Santos stated that the project aims to train around 6000 specialists with cybersecurity skills[201], while Brigadier General Paulo Viegas Nunes stated that the project aims to train over 10,000 specialists with cybersecurity skills by 2030[202]. The official number stated in the CNCS website, however, is at least 9800 specialists by the first trimester of 2026[203]. Lastly, the fourth and fifth axes foresee the necessity for national participation in the various existing *fora* in the field of cyberspace and cyberspace security, which would allow Portugal to not fall behind and bring in new solutions or present new solution within said *fora*. This would establish independence in this particular field. [204]

[200] Portuguese Republic, "ANNEX - National Strategy for Cyberspace Security 2019-2023," in *Portuguese Official Journal*, vol. 108 (Imprensa Nacional, 2019), 2894.
[201] António Miguel Neves Almeida and Lino Santos, Interview: Coordinator Lino Santos, personal, February 13, 2023. Refer to Appendix III, p. 203.
[202] António Miguel Neves Almeida and Paulo Viegas Nunes, Interview: Brigadier General Paulo Viegas Nunes, personal, January 13, 2023. Refer to Appendix I, p. 157-8.
[203] CNCS, "C-Academy," CNCS, accessed February 24, 2023, https://www.cncs.gov.pt/pt/c-academy/.
[204] Portuguese Republic, "ANNEX - National Strategy for Cyberspace Security 2019-2023," in *Portuguese Official Journal*, vol. 108 (Imprensa Nacional, 2019), 2893-4.

The sixth and final axis of the Portuguese Cyberspace Security Strategy is entitled "National and International Cooperation". It sets out various goals to deepen national cooperation and participation within international organizations, notably with the United Nations, the European Union, NATO, and OSCE. This participation can come in the form of participation in war games and other exercises in order to increase the level of maturity and preparedness, specifically in the cybersecurity and cyber defence areas. It can also come in the form of deepened cooperation between national entities in this area with the goal of having a more effective alert and response framework, as well as integrating international cybersecurity and defence organizations with Portugal's own national entities. Finally, Portugal seeks to affirm itself within cyber diplomacy, exchanging best practice behaviours within cyberspace to which it should adhere to, as well as contributing to the regulation and universalization of cyberspace by encouraging compliance with international law that is relevant to this specific area.[205]

[205] Ibid., 2894.

5. The Threats to NATO in Cyberspace

We have seen throughout recent years how cyber threats have not only increased in number, but also in scale and sophistication. As advanced economies increasingly shift their activities online, societies face the very real possibility and danger of certain aspects of cyberspace becoming weaponized. This weaponization can involve manipulating perceptions and opinions, influencing public sentiment, and targeting governments, industries, and individual citizens alike. Moreover, in terms of impact, appropriately employed cyber capabilities possess the potential to cause tangible harm, neutralize, or even dismantle specific critical infrastructures such as telecommunications centres or nuclear plants.[206] We will take a look at a few key examples that challenge – and will continue to challenge – NATO and its member-states in the years to come. These cyber threats can come from different sources, both state and non-state actors, as well as state-sponsored actors. The main actors that threaten NATO and its members are Russia and China, each in different ways, both of which will be looked at in more detail further ahead. The main types of cyber threats explored in this chapter, will be disinformation and misinformation, intellectual property theft and cyber-espionage, critical infrastructure as a cyber target, and false-flag/no-flag cyber-attacks. We will examine how foreign superpowers such as China and Russia take advantage of cyberspace to achieve their own objectives, prioritizing certain elements to advance their own arsenal or to disrupt their geopolitical competitors, and how cyber weapons created by the NATO members can later, and inevitably, be used against NATO and its members.

[206] Manuel Poêjo Torres, William Hasselberger, and Francisco Proença Garcia, "The Atlantic Posture and the 'Cybrid' Threats of Tomorrow," essay, in *O PODER AUTORITÁRIO E O DESAFIO PARA AS DEMOCRACIAS LIBERAIS* (Óbidos, Portugal: Alêtheia Editores, 2022), 130–69, 145.

5.1. Disinformation & Misinformation

We will begin by exploring the aspect of disinformation. It is the action of disseminating misleading or outright false and manipulated information throughout cyberspace to create instability and mistrust among the general populace of a targeted country/bloc, and it is an aspect that has become a challenge for NATO and its member-states and will only become an even greater challenge as tactics and methods become increasingly sophisticated; for example, how today video and audio can be manipulated into a "deep fake" and mimic the likeness and voice of a world leader. This form of cyber threat is one that does not depend upon directly attacking a target, but rather, introducing ideas into the grid that is cyberspace, which can have varying results, some greater than others, as we have already seen in the past, and for that reason it can be as dangerous, or more so, as a direct cyber-attack. According to Rear-Admiral António Gameiro Marques, our biggest threat "*is the way some states or state-sponsored actors deliberately try to alter our perception of the world*"[207]. It is also important to note that this cyber threat also presents a danger to authoritarian and totalitarian regimes, where freedom of speech is limited or non-existent, as it can serve as a means to bypass censorship, combat oppression, and facilitate the organization of protests,[208] as we saw with the Arab Spring for example.

Disinformation is usually disseminated through social networks, where content – some of it unverified – is shared without restriction. This is only aided by the fact that many users lack the knowledge and knowhow of how the internet works, of what is at stake, and that everything online may not be the truth, may not be facts. To "*effectively counter international*

[207] António Miguel Neves Almeida and António Gameiro Marques, Interview: Rear-Admiral António Gameiro Marques, personal, January 23, 2023. Refer to Appendix II, p. 176.
[208] Manuel Poêjo Torres, William Hasselberger, and Francisco Proença Garcia, "The Atlantic Posture and the 'Cybrid' Threats of Tomorrow," essay, in *O PODER AUTORITÁRIO E O DESAFIO PARA AS DEMOCRACIAS LIBERAIS* (Óbidos, Portugal: Alêtheia Editores, 2022), 130–69, 147.

disinformation, one needs to first recognize it,"[209] and users may not know how to spot fake news, either by checking the origin or the content within, conducting a more thorough fact checking from other sources. This method of dissemination of disinformation relies greatly on that aspect, that the user will neglect the necessary caution and disseminate that news across cyberspace, in essence, exploiting one of the weakest links of cyberspace – users.

We have already seen examples of these disinformation efforts carried out by China[210] and especially by Russia[211], where "*disinformation has become a matter of established policy*"[212] and has affected NATO member-state, such as the United Kingdom with Brexit, and the United States of America with its 2016 Presidential Elections. Both had similar *modi operandi* when it comes to the false or misleading information disseminated throughout the web.

With regards to Brexit, false or inaccurate data was spread through social media and even by politicians campaigning to leave the European Union, with the campaign being described as "*divisive, antagonistic and hyper-partisan*"[213]. Among the disseminated false information was that the UK sent £350 million per week to the European Union, when in reality this figure did not include the rebate, so *"[i]n 2014 the UK would have paid £18.8 billion without the rebate but ended up paying £14.4 billion. The estimate for 2015 is £12.9 billion. This is £248 million per week, or £35 million per day*"[214]; another bit of false information was that the net migration to the UK had hit 333,000, and that Turkey was going to join the EU

[209] André W.M. Gerrits, "Disinformation in International Relations: How Important Is It?," *Security and Human Rights* 29, no. 1–4 (2018): 3–23, https://doi.org/10.1163/18750230-02901007, 13.
[210] Manuel Poêjo Torres, William Hasselberger, and Francisco Proença Garcia, "The Atlantic Posture and the 'Cybrid' Threats of Tomorrow," essay, in *O PODER AUTORITÁRIO E O DESAFIO PARA AS DEMOCRACIAS LIBERAIS* (Óbidos, Portugal: Alêtheia Editores, 2022), 130–69, 142.
[211] Ibid., 156-7.
[212] André W.M. Gerrits, "Disinformation in International Relations: How Important Is It?," *Security and Human Rights* 29, no. 1–4 (2018): 3–23, https://doi.org/10.1163/18750230-02901007, 10.
[213] Hannah Marshall and Alena Drieschova, "Post-Truth Politics in the UK's Brexit Referendum," *New Perspectives* 26, no. 3 (2018): pp. 89-105, https://doi.org/10.1177/2336825x1802600305, 94.
[214] Ibid., 94.

relatively soon and that its workers would flood the UK labour market, leaving many British nationals unemployed, when in reality, in the best case scenario, Turkey would only join the EU a few decades from now. Another element in the dissemination of false information is the use of "bots" throughout several social media platforms. Bots are essentially programs that autonomously carry out instructions, and in this particular case the instructions were to share this false or misleading information throughout those social media platforms. Bots can share and generally disseminate false information much faster than a human "troll" having to do it manually, increasing the overall success of the dissemination. According to data from Twitter, the #voteleave had a substantially higher count than the #remain, as we can see in *Figure 7*[215]. As mentioned above, social media networks are one of, if not the, main way to disseminate fake news stories; in the UK 64% of adults use the internet to as the main source for their news, with the number increasing to 82% in regards to people aged between 16-24 years of age. Likewise, 44% of UK adults use social media to gain access to their news stories. These figures show us that the susceptibility of users falling victim to false information and subsequently sharing said false information is within a probable degree, at least in regards to Brexit in the UK, with a possible transposition to more divisive (future) topics.[216]

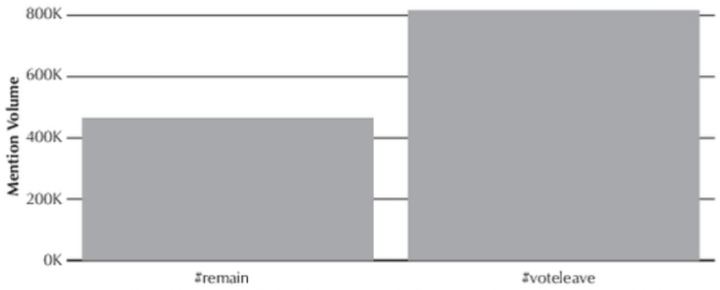

Figure 7: EU Referendum - Remain vs. Leave related hashtags (8th May - 7th June)

With regards to the United States, misinformation was disseminated throughout the web during multiple occasions, such as presidential and mid-term elections, but the most prominent example – and one might argue the most successful example – was the 2016 Presidential

[215] Ibid., 95.
[216] Ibid., 96.

Election between republican candidate Donald Trump, and Democrat candidate Hillary Clinton.[217] The overall objective of this disinformation campaign – codenamed "Project Lakhta"[218] – perpetrated by the Russian Government was to harm the candidacy of democrat candidate Hillary Clinton, while also boosting the candidacy of republican candidate Donald Trump, while also increasing the level of discord and mistrust among the US population, having been ordered, according to US intelligence, by Russian President Vladimir Putin. Project Lakhta was not created for the sole purpose of interference in this particular election, but rather as an ongoing campaign of interference and information warfare targeting the United States especially.[219] Through the Internet Research Agency (IRA), essentially a Russian "troll farm", the Russians were able to disseminate large amounts of false content through millions of social media users, again, with the goal of supporting Trump, and to disparage Clinton. Aside from the IRA, other elements of Russian intelligence stole and leaked files and emails from the Democratic National Committee and the Clinton campaign, releasing them on various websites, such as the notorious WikiLeaks website. According to the Report on the Investigation into Russian Interference in the 2016 Presidential Election (often called the "Mueller Report", named after the Special Counsel who led the investigation, Robert Mueller) states that the IRA used a wide array of social media platforms to disseminate their content, among them: Facebook, Twitter, Instagram, Reddit, YouTube, among others. Regarding Facebook the report states the "*a Facebook representative testified that Facebook had identified 470 IRA-controlled Facebook accounts that collectively made 80,000 posts between January 2015 and August 2017. Facebook estimated the IRA reached as many as 126 million*

[217] Manuel Poêjo Torres, William Hasselberger, and Francisco Proença Garcia, "The Atlantic Posture and the 'Cybrid' Threats of Tomorrow," essay, in *O PODER AUTORITÁRIO E O DESAFIO PARA AS DEMOCRACIAS LIBERAIS* (Óbidos, Portugal: Alêtheia Editores, 2022), 130–69, 146.
[218] "Russian Project Lakhta Member Charged with Wire Fraud Conspiracy," *Department of Justice*, September 10, 2020, https://www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy.
[219] Rachel Weiner, "Russian National Accused of Fraud Conspiracy Aimed at Political Interference," *Washington Post*, September 10, 2020, https://www.washingtonpost.com/local/legal-issues/russian-national-accused-of-fraud-conspiracy-as-part-of-election-interference/2020/09/10/abfda006-f370-11ea-bc45-e5d48ab44b9f_story.html.

persons through its Facebook accounts"[220]; regarding Twitter the report states that "*Twitter announced that it had identified 3,814 IRA-controlled Twitter accounts and notified approximately 1.4 million people Twitter believed may have been in contact with an IRA-controlled account*"[221], adding that "*IRA-controlled Twitter accounts separately had tens of thousands of followers, including multiple U.S. political figures who retweeted IRA-created content*"[222], with multiple IRA-controlled Instagram accounts having hundreds of thousands of U.S. followers.[223] Also noteworthy is the fact that the IRA focused on mainly on national and security issues, while only 11% of their social media content focused on the election itself. These included, among others, veterans' issues, gun rights, racial issues (particularly African American issues), minority issues, feminism, and patriotism in general, going so far as spreading content related to succession movements in California. Again, we can deduce by the content that was disseminated that the goal of the IRA was to sow division and discord in American society.[224] Disinformation and misinformation exploit these societal differences and divisions, and all these issues are hot button issues that, when taken to an extreme, can cause a strong divisive force and polarise society to a point where no common ground can be reached. This mistrust and division also extend to the trust in media and the government, which may lead people to become more susceptible to this sort of false or misleading content, and why "*media campaigns by governments and other initiatives […] that are supposed to distinguish*

[220] Robert S. Mueller, Report on the investigation into Russian interference in the 2016 presidential election: Submitted pursuant to 28 C.F.R. §600.8(c) § (2019), https://www.justice.gov/archives/sco/file/1373816/download, 23.
[221] Ibid.
[222] Ibid.
[223] Ibid.
[224] Alex Ward, "4 Main Takeaways from New Reports on Russia's 2016 Election Interference," *Vox*, December 17, 2018, https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

reliable media from untrustworthy ones, may not be particularly effective".[225] This exploitation of freedom of speech in democracies will be an issue touched further ahead in this thesis.

To help counter this particular threat and its varying impacts, many national governments have taken a range of steps. These steps include the establishment of networks, task forces and working groups, strategic communication units, as well as other institutions dedicated to this issue. Likewise, some governments have updated existing laws or created new ones, and others have focused on collaborating with social network companies to regulate the content published on these platforms.[226] However, the issue is a complex one, and may require more extensive actions to help reduce its effects in the long term, as we shall see ahead.

5.2. Intellectual Property Theft & Cyber-Espionage

Another threat that we must look at is that of intellectual property theft; this can be defined essentially as the theft of an individual's or company's ideas and/or inventions; this can include trade secret theft and patent infringement. This form of cyber threat can be quite challenging to counter as the number of methods that exist to gain unauthorized access can vary, some of which have already been touched on earlier in this thesis; phishing, trojan horse attacks and spyware are examples of this. It is important to note that the methods used to gain unauthorized access in cyber-espionage are different from those used outside cyber-espionage; the main characteristic here is that with cyber-espionage, one does not want to alert the target of their presence or that they have gained unauthorized access, and so for that reason typical trojan attacks may not be ideal to achieve these objectives. One of the methods used to gain access is through a system or network backdoor; these backdoors are created and inserted by hardware/software engineers into their systems in the event users are locked out of said system.

[225] André W.M. Gerrits, "Disinformation in International Relations: How Important Is It?," *Security and Human Rights* 29, no. 1–4 (2018): 3–23, https://doi.org/10.1163/18750230-02901007, 14.
[226] Ibid., 15.

These backdoors can be used by hackers as an entry point into the system, or they may be created by said hackers that found a vulnerability within the system itself. Once the intruder has gained access to the system they are able to mine the network for credentials of authorized users, and in that manner they can use those credentials to gain access to different parts of the system undetected, and gain access to its most valuable data. Another method is finding and taking advantage of an unwitting accomplice, usually done using the aforementioned "phishing" method. These methods may vary slightly but may include posing as a known associate of the accomplice and sending them an email or message with a link containing malicious code that will allow the hacker access into the network and the ability to mine and exfiltrate any relevant data. Exfiltrating that amount of data would cause suspicion, so, in order to conceal the extraction of data and avoid detection, hackers will employ techniques such as fragmenting data into smaller files and camouflaging the data flow within legitimate network traffic.[227]

While this may appear to be a secondary issue that wouldn't affect NATO or its security, in reality it can have long term and indirect effects on NATO, especially when the intellectual property being stolen concerns defence systems, inside or outside of cyberspace. One notorious practitioner of this tactic is China, which we will be exploring. China is the U.S.' – and by extension, the West's – most formidable adversary, both economically and militarily, and, more concerning to us, in cyberspace. China was one of the first major powers to recognize the importance of cyberspace and the potential role it might play in warfare and in daily life. This was touched upon by two Chinese Colonels of the PLA (People's Liberation Army) Qiao Liang and Wang Xiangsui in their 1999 book "Unrestricted Warfare", where they state that "*[t]oday, with information technology welding the entire world together into a network, the*

[227] Jeffrey B. Jones, "Confronting China's Efforts to Steal Defense Information," Harvard Kennedy School Belfer Center for Science and International Affairs, May 2020, https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.

number of factors involved in a war is much, much greater than in past wars"[228]. They argued that in the future, traditional military tactics and strategies may no longer be effective, and that non-military means, such as economic or cyber warfare should be explored in conjunction with traditional military strategy; they explain that cyber capabilities – or as they call it "information technology" – can and should be used to "*shrink the course of warfare*"[229], and that this would enable asymmetrical warfare that would allow China to gain the upper hand against the U.S. and the West.

When it comes to intellectual property theft, China has been particularly active in their cyber-espionage, especially in certain areas they deem critical to its economic and national security objectives. To give an example of this, between 2010 and 2015, state-sponsored Chinese hackers targeted both U.S. and European aerospace companies, stealing relevant information that China then used to develop its state-owned aerospace industry. In 2018, when this was discovered, Chinese companies had already used that information and had already built commercial jets based in part on the stolen intellectual property. This has been an ongoing issue, and to this day China, or rather, its state-sponsored actors have continually targeted a multitude of companies and institutions working in strategically relevant areas, such as medical institutions, semiconductor firms, and most importantly (for NATO): defence.

Just like China did between 2010 and 2015 when they used Western intellectual property they stole to develop their own industry, they will, likewise, do the same when it comes to defence. This has led leaders in the West to denounce and condemn these activities, officially calling on China to help halt these attacks perpetrated on Chinese soil. In July 2021 the European Union's High Representative Josep Borrell in statement exposed several malicious cyber activities originating from Chinese territory. He stated that some of these

[228] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House Arts, 1999), 215.
[229] Ibid., 207.

attacks affected government institutions, political organizations and private companies, specifically key industries within the EU. According to the statement, these attacks are perpetrated by hacker groups known as Advanced Persistent Threat 40 and Advanced Persistent Threat 31, with the purpose of intellectual property theft and espionage.[230]

As we can see, intellectual property theft and cyber-espionage can become a greater threat to NATO and the West than it may initially appear, which is why many of these key private companies are also now investing greatly in their own cybersecurity, as mentioned earlier. While these attacks may not be so publicly spoken of in the media, they are no less relevant or dangerous to a nation's national cybersecurity. This fact may, however, have a negative effect; if instances like this are not adequately reported, policymakers may fail to give the issue the attention it deserves, and, likewise, may result in policy makers lacking a certain level of understanding needed to make decisions concerning these issues. In other instances, many key industry sectors may not reveal these breaches either due to the companies in question not wanting to divulge said breaches for fear of having their public image and standing damaged, resulting in the erosion of their business and financial gains, or due to the nature of cyber-espionage resulting in many of these breaches going undetected. Similarly, governments may not wish to disclose breaches either because it may reveal their sources or the methods used to obtain that information, or because they may wish to let such breaches unfold so that they may learn how a rival operates, allowing for better insight and therefore improved countermeasures, and overall security, in the future. As previously mentioned, China not only engages in the theft of sensitive defence data but also collaborates with its defence industry to integrate the acquired knowledge into the development of its own advanced weapons platforms.

[230] "China: Declaration by the High Representative on Behalf of the European Union Urging Chinese Authorities to Take Action against Malicious Cyber Activities Undertaken from Its Territory," *European Council*, July 19, 2021, European Union, https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/.

This mutually beneficial relationship enables China to create replicas of vital U.S. weapon systems, such as Lockheed Martin's F-22 Raptor and F-35 Joint Strike Fighters. In the U.S. alone Chinese cyber-espionage has resulted in an estimated loss of around $300 billion per year.[231]

While many solutions to prevent this can be proposed – solutions such as data obfuscation (the process of making data obscure or unintelligible), incentivising private companies to invest in their cybersecurity, or designing intrusion detection systems to identify anomalous network traffic or recognize the distinct patterns associated with known malicious actors – none are truly fool-proof, and can be circumvented given enough time and/or resources. The only way one can keep truly keep a network from being hacked remotely is by cutting it off completely from the internet. "*This can be done without eliminating the highly desirable collaborative benefits of the connected networks. By implementing a controlled number of highly secured and heavily monitored gateways, a company can reduce the number of nodes to protect.*"[232] It is, however, important to note that even in an isolated system, the presence of an insider with direct access to the computer network can still render it susceptible to exploitation.[233]

5.3. Targeting Critical Infrastructure

Critical infrastructure is an alluring target for cyber actors that may seek to cause disarray or destruction. With a growing dependence and interdependence on cyberspace and in each other, critical infrastructure has increasingly become a target; but what is critical infrastructure, and how can we define it? Critical infrastructure is considered critical when its

[231] Jeffrey B. Jones, "Confronting China's Efforts to Steal Defense Information," Harvard Kennedy School Belfer Center for Science and International Affairs, May 2020, https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.
[232] Ibid.
[233] Ibid.

potential disruption has the ability to significantly impact social stability and the sovereignty of a nation, and may include water and power distribution, (nuclear) power plants, telecommunications, transport systems such as railways, food and agriculture, and sewage and garbage disposal.[234] As previously mentioned, essential services can also be considered as part of critical infrastructures, which may include – but is not limited to – health and emergency services, tax authority, social security, ministries' networks, and assets databases.[235] As we can see, modern society is dependent on critical infrastructures, which, in turn, rely on each other for their proper functioning. This growing interconnection and interdependence have been identified and raised as a significant cause for concern. The probability of a minor incident setting off a chain reaction of events with far-reaching consequences has increased significantly.[236]

To understand why critical infrastructure protection is essential we must first look at the technical aspect of the matter. Critical infrastructure – the industrial type to be more specific – is generally operated by what is known as industrial control systems that oversee said operations and manage physical equipment such as pumps, motors, and a wide array of sensors, among other aspects.[237] One of these systems is SCADA (Supervisory Control and Data Acquisition), and it "*consists of both software and hardware components and enables remote and on-site gathering of data from the industrial equipment. In that way, it allows companies to remotely manage industrial sites such as wind farms, because the company can access the*

[234] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014), https://www.revistamilitar.pt/artigo/913.
[235] António Miguel Neves Almeida and Paulo Viegas Nunes, Interview: Brigadier General Paulo Viegas Nunes, personal, January 13, 2023. Refer to Appendix I, p. 152-3.
[236] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014), https://www.revistamilitar.pt/artigo/913.
[237] Stuart Collins, "Cyber Attacks on Critical Infrastructure," AGCS Global, June 2016, https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

turbine data and control them without being on site."[238] To put it simply, the management of nearly all industrial critical infrastructures today is conducted remotely from control rooms utilizing computers and communication networks; in essence, IT systems. These infrastructures encompass a range of operations, from overseeing chemical manufacturing processes and railway signalling, to managing power grids and other aspects as mentioned earlier. It is important to note that SCADA systems can automatically adjust the different phases of production or maintenance via data gathered from relevant sensors, down to the minutest detail, and regardless of the proximity or geographic distance, it has the capability, through cyberspace, to accomplish this task.[239] This aspect is essential to understanding why critical infrastructure protection is of great importance, and why it must be taken with all seriousness.

By 1995, the United States was aware that the dependence of critical infrastructure on information networks, notably the internet, was increasing, and this became a growing concern as they could become vulnerable to attacks coming from cyberspace. In the past, critical infrastructure systems were physically isolated, which made them less appealing to hackers. However, with the interconnection of information networks such as the internet, critical infrastructure systems are now more exposed to attacks as many of them are connected to the internet and use commercial off-the-shelf (COTS) software and standard operating systems. The linkage of these SCADA systems to the internet has significantly increased, exposing systems that were, in a sense, never designed to be connected to public networks. Additionally, many communication protocols used in critical infrastructure systems were designed without authentication or encryption, making them now susceptible to cyber-attacks, and the lack of

[238] SCADA International, ed., "Learn All about SCADA Systems: What Is SCADA?: Scadapedia," SCADA International, April 20, 2023, https://scada-international.com/what-is-scada/?utm_medium=cpc&utm_source=google.com&utm_campaign=scada-explained&gad=1&gclid=CjwKCAjwpayjBhAnEiwA-7ena7ZeocaHWLY53gJfOGz5AqmJXX8lfJz7yD9E7-kHVUTN09svXBmOtBoCjfkQAvD_BwE.

[239] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014), https://www.revistamilitar.pt/artigo/913.

regular security updates is also a problem, as interrupting the operation of a SCADA system to install updates can be economically unfeasible. Another factor that can contribute to the vulnerability of critical infrastructure systems is that of mobility, this is because technicians can use personal devices to remotely monitor and control these systems. This introduces the risk of malware inevitably infecting the systems through insecure applications. Furthermore, many private companies operating and managing critical infrastructure systems may not adequately prioritize security, which calls back to earlier, where private companies may not have the incentives to invest and upgrade their cybersecurity. In essence: *"[m]any [Industrial Control System] components are connected to the Internet without proper security*."[240] Another concerning issue regards the acquisition of hardware from dubious sources, such as China, which has, on multiple occasions, raised doubts on the reliability of hardware and components they supply to the world, especially when it comes to using said hardware – and software – for spying.[241] Vulnerabilities in these components have only increased throughout the years, with 672 reported in 2018, 716 in 2019, and 893 in 2020; furthermore, these numbers do not include common ICT components, such as employee's personal phones or computers.[242]

When we think of a cyber-attack against critical infrastructure, we may think of Stuxnet, a sophisticated cyber weapon believed to have been developed by the United States and Israel, that was used in 2010 against the Islamic Republic of Iran and serves as a quintessential instance of an attack on critical infrastructure. It was used to severely disrupt Iran's nuclear program by targeting the nuclear centrifuges at the Natanz nuclear facility which were used to

[240] Sungbaek Cho, "Enhancing Cybersecurity of Industrial Control Systems," essay, in *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)*, ed. USAWC Press (Carlisle, PA: Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022), 355–85, 362.
[241] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014), https://www.revistamilitar.pt/artigo/913.
[242] Sungbaek Cho, "Enhancing Cybersecurity of Industrial Control Systems," essay, in *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)*, ed. USAWC Press (Carlisle, PA: Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022), 355–85, 361-2.

enrich uranium. Specifically, Stuxnet targeted the facility's programmable logic controllers (PLCs) – another type of process control similar to SCADA which functions as a specialized industrial computer designed to control and automate manufacturing processes and is specifically built to withstand harsh industrial environments – and as a result the system was deceived into believing that the centrifuges were operating at their intended speed. However, the controller was being manipulated, causing the centrifuges to spiral out of control until they exceeded their physical limits, resulting in their ultimate breakdown.[243]

This is only one of the few attacks that is divulged to the public; other examples include Havex in 2013 which affected several NATO member-states, the Ukraine Blackout in 2015, TRITON in Saudi Arabia (2017), and the Colonial Pipeline in the United States (2021).[244] It is possible that we remain unaware of other such attacks that may have happened. Naturally, this attack has opened a veritable Pandora's box. It has raised concerns not only due to the adaptability of Stuxnet to target SCADA systems, which are extensively employed in critical infrastructure and manufacturing industries across Europe and the United States, but because Stuxnet and its subsequent variations brought SCADA systems to the forefront, revealing their vulnerabilities and generating a pervasive feeling of insecurity concerning global critical infrastructures. Ever since then the frequency of attacks targeting critical infrastructures in the United States alone has experienced a significant exponential rise, going from 39 attacks in 2010 to 198 attacks in the following year, little under a 408% increase in one year, and later decreasing to 138 attacks in 2012.[245]

---

[243] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014), https://www.revistamilitar.pt/artigo/913; António Miguel Neves Almeida and António Gameiro Marques, Interview: Rear-Admiral António Gameiro Marques, personal, January 23, 2023. Refer to Appendix II, p. 180.

[244] Sungbaek Cho, "Enhancing Cybersecurity of Industrial Control Systems," essay, in *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)*, ed. USAWC Press (Carlisle, PA: Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022), 355–85, 365-9.

[245] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014),

The impact of a cyber-attack on critical infrastructure can vary significantly. While a successful attack usually does not result in human casualties, it can cause service disruptions. This can encompass disruptions in telecommunications, internet service providers, and network outages that can impact a significant portion of public sector services. However, an attack on the control systems of a chemical facility for example can cause a greater amount of damage over a wide area. These consequences can range from relatively harmless temporary disruptions to deliberate acts of sabotage intended to cause a large number of victims, such as explosions in industrial facilities. A cyber-attack that affects a critical infrastructure may not only impact its business sector but also have implications for public health, the economy, and national security, and all these sectors may be affected one after the other successively, like falling dominos. For example, by 2030, it is projected that the UK economy will heavily rely on digital technologies, accounting for approximately 70% of its overall structure.[246] This significant digital dependency implies that any disruption or adverse impact on the digital infrastructure could potentially inflict substantial harm on the UK as a whole. Another area of concern that has already been mentioned is the national power grid, which has dual use, supplying both the public and private sectors. An attack on a critical point in the power grid can shut down sectors that supply hospitals and military bases simultaneously. Targeting the power grid can be an effective way to weaken a nation's military capacity as the existence of multiple vulnerabilities and a complex network of interdependencies among critical infrastructures contribute to a situation where an attack on a critical infrastructure can have a significant impact on those who depend on it.[247]

---

https://www.revistamilitar.pt/artigo/913; Stuart Collins, "Cyber Attacks on Critical Infrastructure," AGCS Global, June 2016, https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

[246] António Miguel Neves Almeida and Paulo Viegas Nunes, Interview: Brigadier General Paulo Viegas Nunes, personal, January 13, 2023. Refer to Appendix I, p. 152.

[247] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014), https://www.revistamilitar.pt/artigo/913.

The increasing dependence of critical infrastructures on technology and their complex interconnectivity heighten vulnerability to cyber-attacks. Although the risk of coordinated attacks against critical infrastructures is generally low, the impact can be extremely high due to the difficulty of recovery and existing interdependencies. Modern society, highly industrialized and dependent on complex infrastructures, is sensitive to disruptions in these infrastructures, and the impact of a disruptive incident can be disproportionately severe. Risk management in industrial control systems is even more challenging due to the complexity of the business and political environment, where many of these systems are beyond the jurisdiction of the governments that depend on them. While there is a demonstration of awareness of existing risks, financial pressures lead organizations to accept high levels of risk in order to maintain their profit margins, resulting in reduced investments in vulnerability reduction, transferring the responsibility for cybersecurity to governments and postponing the implementation of security measures.[248]

Completely protecting a system from all threats is impossible, so it is necessary to adopt a holistic risk management approach that balances resilience, restoration, and protection. This includes context establishment, risk identification, risk analysis, risk evaluation, and risk treatment.[249] Other simple cybersecurity steps include the frequent and regular backing up and patching of systems, scanning and managing incoming and outgoing data and emails, enforcing security across the entirety of the supply chain, and establishing and incident response plan.[250] The potential cascading impact of a cyber-attack on critical infrastructure within a nation places it at the forefront of priorities for individual governments and NATO when addressing cybersecurity and (cyber) defence concerns. As mentioned several times throughout this thesis,

[248] Ibid.
[249] Sungbaek Cho, "Enhancing Cybersecurity of Industrial Control Systems," essay, in *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)*, ed. USAWC Press (Carlisle, PA: Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022), 355–85, 373-5.
[250] Ibid., 369-70.

it has been repeatedly emphasized that private entities may choose not to prioritize their own cybersecurity investments, instead relying on the state to handle this responsibility, allowing them to maintain an increased profit margin. To ensure an acceptable level of cybersecurity, governments need to establish mandatory security requirements and minimums for companies operating critical infrastructure, making regular inspections to guarantee that these requirements are met, while also providing security advice when required.[251] However, in some cases companies hold the belief that the government lacks the capability to ensure their cybersecurity effectively, and as such, they perceive the associated risks as justifiable and deem investing in cybersecurity to be worthwhile. According to the AGCS "*the economic and insurance impact of a severe, yet plausible cyber-attack against the US power-grid to total in excess of $240bn, possibly even rising to more than a $1trn.*"[252] This is why the power sector has taken the lead in addressing these concerns globally. Despite its significant reliance on other infrastructures, the power sector is often regarded as *primus inter pares* because of its central role in industrial control systems.[253]

Improving management and risk activities across all industrial control systems is a major priority for the future. Since the interconnected nature of these industrial control systems prevents isolated sector analysis, methodologies aligned with international standards – such as the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards, or the ENISA's "Protecting Industrial Control Systems" – need to be adopted

[251] Ibid., 384.
[252] Stuart Collins, "Cyber Attacks on Critical Infrastructure," AGCS Global, June 2016, https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.
[253] Rui Manuel Piteira Natário and Paulo Fernando Viegas Nunes, "RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS," *Revista Militar*, no. 2547 (April 2014), https://www.revistamilitar.pt/artigo/913.

worldwide to address the challenges and help mitigate the risks posed by malware such as Stuxnet and its subsequent iterations.[254]

5.4. False-flag & No-flag Cyber-Attacks

Perpetrators of cyber-attacks often opt not to claim credit for their actions. This may occur when they desire to maintain secrecy, fear facing retaliation, or anticipate adverse repercussions from public backlash; and in some cases, they wish to create the illusion that the attack was orchestrated by a different party. This is what is known as no-flag attacks and false-flag attacks respectively, and in those cases attribution in the cyber domain can be a complex process, and operations such as these further complicate the task of identifying the true origin and motives behind a cyber-attack. Investigators often need to rely on a range of technical indicators, behavioural patterns, intelligence sources, and collaboration with international partners to ascertain the responsible party, and even with these efforts, achieving a high degree of certainty in attribution is not always possible. It is important to note that these types of cyber threats are not of a distinct category of cyber threat that differ from the last three we have analysed; however, their nature is an important aspect that must be looked at to understand the complexity of cyberspace and cyberspace security.

False-flag (and no-flag) attacks are employed both inside and outside of cyberspace, with the expression originating in 16th century maritime warfare, whereby a vessel would fly the flag of an enemy or neutral nation in an attempt to deceive or hide their true identity.

[254] Sungbaek Cho, "Enhancing Cybersecurity of Industrial Control Systems," essay, in *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)*, ed. USAWC Press (Carlisle, PA: Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022), 355–85, 370-2.

5.4.1. False-flag Cyber-Attacks

False-flag cyber-attacks do not differ greatly from this explanation; they can be defined as incidents where in which a perpetrator disguises their identity or intentionally attributes the attack to another entity.[255] The purpose is to deceive and/or mislead investigators, making it appear as if a different entity was responsible for the attack; the entity might use various techniques to create the false impression of attribution, such as altering the attack's digital fingerprints, mimicking the language and writing style of a different group, modifying or forging digital evidence such as IP addresses, timestamps, malware signatures, utilizing specific tools or tactics, techniques, and procedures associated with another group, or manipulating the attack's indicators of compromise or IOCs – which refer to data that indicates if a system may have been infiltrated by a cyber threat – to point towards a different origin. The motivations behind false-flag cyber-attacks can vary but are often driven by political or strategic objectives. They may be employed for political reasons, to create diplomatic tensions between nations, incite conflicts, influence public opinion against a particular entity, create confusion and ambiguity, or simply to evade consequences and potentially manipulate the narrative surrounding the attack.[256]

One notable instance of a false-flag attack occurred in 2019 when the suspected Russian-based cyber espionage group "Turla", which has a history of employing sophisticated tactics to achieve their objectives, disguised themselves as Iranian state-sponsored hackers and managed to infiltrate networks in over thirty countries. Unbeknownst to the Iranian government, Turla managed to acquire Iranian cyber tools

[255] Mauno Pihelgas, ed., "Mitigating Risks Arising from False-Flag and No-Flag Cyber Attacks," CCDCOE, March 31, 2015, https://ccdcoe.org/uploads/2018/10/False-flag-and-no-flag-20052015.pdf, 6.
[256] Florian Skopik and Timea Pahi, "Under False Flag: Using Technical Artifacts for Cyber Attack Attribution," *SpringerOpen* 3, no. 8 (March 20, 2020), https://doi.org/https://doi.org/10.1186/s42400-020-00048-4.

– Neuron and Nautilus – and use these to achieve their objectives. The specific methods and tools employed by Turla to mimic Iranian cyber operations was done so to leave behind digital fingerprints and indicators that pointed towards Iran, exploiting the geopolitical tensions and complex attribution challenges in the cyber realm and creating a misleading trail for investigators to follow.[257]

5.4.2. No-flag Cyber-Attacks

No-flag cyber-attacks are similar to false-flag attacks, except with a small difference. Where one seeks to masquerade as a third party (false-flag), the other seeks to keep their involvement a secret (no-flag). No-flag attacks are incidents where the identity or attribution of the attacker is intentionally obscured or hidden.[258] In these cases, it is challenging to determine the true source of the attack or the motives behind it. No-flag attacks often employ advanced encryption and secure communication channels to prevent interception and analysis and intricate layers of obfuscation to hide the true identity of the attackers. They may route their attacks through multiple compromised systems or utilize anonymization techniques like TOR (The Onion Network) to mask their IP addresses or using code signing certificates stolen from legitimate entities. This complexity poses significant challenges for investigators, making it exceedingly difficult to accurately trace the origins of such attacks.

No-flag cyber-attacks can be conducted by states, state-sponsored actors, criminal organizations, and hacktivist or hacker groups. The objective is to avoid detection, evade attribution, and minimize the risk of retaliation or legal consequences. The motivations behind no-flag cyber-attacks can vary widely, but state-sponsored

[257] National Cyber Security Centre, GCHQ § (2019), https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims.
[258] Mauno Pihelgas, ed., "Mitigating Risks Arising from False-Flag and No-Flag Cyber Attacks," CCDCOE, March 31, 2015, https://ccdcoe.org/uploads/2018/10/False-flag-and-no-flag-20052015.pdf, 6.

actors may conduct such attacks for intelligence gathering, political manipulation, or disruption purposes while avoiding retribution. We have already discussed instances such as these in this chapter, such as in cases where China engaged in cyber-espionage, stealing intellectual property for economic and political purposes. Criminal organizations are cyber actors that might employ no-flag tactics to carry out financially motivated cybercrimes without being easily identified, and in some cases, individuals with advanced hacking skills may engage in no-flag attacks for personal reasons or to prove their abilities without being detected.[259] An example that can be classified as a no-flag cyber-attack, and one we have already looked at in this chapter, is Stuxnet. It can be classified as such due to the fact that the creators of Stuxnet intended to maintain its origins concealed, and it demonstrated the capabilities of a no-flag operation, as the true origin and motivations were not immediately apparent. It took extensive analysis and investigation by cybersecurity experts to uncover the complexity and intended target of the attack.

As we can see, false-flag attacks and no-flag attacks are not a necessarily different category of cyber threats from the previously discussed disinformation/misinformation, cyber-espionage, and critical infrastructure. They are in fact tactics employed to accomplish objectives relating to these aforementioned cyber threats. It can perhaps be argued that, in fact, false-flag and no-flag cyber-attacks are the most troubling, contributing to the most disconcerting scenarios and amplifying the already existing level of unease posed by the aforementioned three cyber-threats.

[259] Florian Skopik and Timea Pahi, "Under False Flag: Using Technical Artifacts for Cyber Attack Attribution," *SpringerOpen* 3, no. 8 (March 20, 2020), https://doi.org/https://doi.org/10.1186/s42400-020-00048-4.

6. Conclusion

Cyberspace is a complex and ever-changing domain in which NATO and other foreign (super) powers operate in, and as we have seen, that complexity has only increased, and as technology becomes more and more sophisticated so too will this complexity increase further within cyberspace, and consequently, for cyberspace security as well. Therefore, one of the fundamental aspects we can conclude from this thesis is that it has become apparent that NATO and its member-states are increasingly falling behind in their ability to keep pace with the relentless advancements witnessed in the ever-evolving domain of cyberspace. This lag poses significant challenges, as the gap between technological progress and cybersecurity and cyber defence capabilities widens, leaving us inadequately equipped to effectively address emerging cyber threats. The consequences of this disparity are far-reaching, as it undermines the collective ability of NATO and its member-states to protect critical infrastructure, national security, and maintain a secure digital environment, for businesses and its citizens to use.

The causes of this have already been examined and explained throughout this thesis. Since cyberspace is characterized by fast-paced technological advancements, where new tools, techniques, and – inevitably – vulnerabilities emerge on a regular basis, keeping up with these rapid changes requires a certain number of elements.

Significant investment in research, development, and training is one such element which some NATO member-states still struggle with due to limited resources they possess, even with the support the Alliance – and other organizations – provides. Cybersecurity investments often compete with other priorities and budgetary allocations within NATO and member-states. Limited funding can impede the acquisition of advanced technologies, recruitment and retainment of skilled personnel, and the establishment of robust cyber defence capabilities. One such example explored is that of Portugal, where its budget constraints have,

in many cases, hindered its cybersecurity and defence capabilities; in one case the Director of the Portuguese National Office of Security (*Gabinete Nacional de Segurança*) Rear-Admiral António Gameiro Marques stated that he was unable to retain talent for a longer period of time, losing them to other international organizations – such as NATO – or to the private sector, as the public sector wages did not allow him to pay these employees higher wages.[260]

This brings us onto the next element, that of talent shortage; this shortage is not limited to Portugal alone, but also to other international organizations such as NATO who struggle to recruit and retain qualified personnel due to intense competition from the private sector and the high demand for cybersecurity experts, which further exacerbates the challenges in keeping pace with the advancements in cyberspace.

Another one of these elements is that of a nation's separation of powers, i.e., the powers of each sovereignty body, and what they can and cannot do. Every NATO member-state exercises its own form of governance. Just because one member-state's sovereign bodies can undertake a particular action, it does not imply that another nation's sovereign bodies can do the same in an identical manner. This is an aspect that can create certain openings in NATO's networks and can hinder NATO's ability to respond to cyber-attacks. We looked at the example of Germany and Spain, where their constitutional limits do not allow them to be as proactive in their cyberspace security. In the case of Germany, we saw how their constitutional limits affect their handling of cyberspace security: the *Bundeswehr* handles cyber defence and the BSI handles cybersecurity; however, they are constitutionally barred from working together. To help prevent cyber-attacks and prevent the setbacks these constitutional restrictions may cause, they depend on their Cyber-AZ, which, as we have seen, functions in an inter-ministerial capacity. When it comes to cyber operations, these must be approved by the *Bundestag* if they

[260] António Miguel Neves Almeida and António Gameiro Marques, Interview: Rear-Admiral António Gameiro Marques, personal, January 23, 2023. Refer to Appendix II, p. 176.

occur on German soil as they fall under the prerogative of the *Bundeswehr*. When it comes to the case of Spain, we have already seen that it is among the Alliance's member-states that recognized the significance of cyberspace at an early stage, and, as a result, made substantial investments in safeguarding that domain. However, while it has invested greatly and has, likewise, taken much of its cyber policies from the European Union's Security Union Strategy, Spain is unable to carry out counterattacks – in the event of a cyber-attack – unless there is an ongoing declared armed conflict. Circumstances such as these can hinder cyberspace security within NATO as it will contrast with those member-states that have a more proactive approach, a less defensive approach, to their cyberspace security, such as the United States, the United Kingdom, and France which we have already looked at in this thesis.

An offensive approach like those taken by the latter three member-states appear to be more effective than the defensive approach taken by the former two. This type of defence forward allows countries to anticipate and strike would-be attackers before they themselves fall victims to a cyber-attack, while also maintaining a level of protection in the event of a cyber-attack; in essence, attacking before they are attacked while also being able to guarantee a sound defence. Countries who rely solely on a more defensive approach, due to their individual national circumstances, will be more susceptible to cyber-attacks, as they can only rely on their defence to keep them from suffering from any cyber-attack. This in turn may create openings in NATO's collective cyberspace security that can be prejudicial. To understand this we may imagine NATO as a castle, but while certain parts of the castle's walls may be well maintained and well defended, other parts may be less defended or fallen into disrepair; these weaker points in the castle's wall – which in this example can be translated to member-states that opt for a defensive strategy – can be seen as an easy target for an attacking force, rather than attacking (more often) the stronger and more well-maintained walls – which in this case can be translated

to those member-states that opt for a more offensive defence, such as the United States or the United Kingdom.

However, circumstances vary from state to state, and in the absence of a uniform strategy, other methods must be used to make up for those less defended or maintained "castle walls" and ensure a more secure Alliance. Methods such as information sharing, done through the MISP (Malware Information Sharing Platform) or the NCIA's Cyber Security Collaboration Hub, which allows a for wide array of information to be distributed throughout the relevant national agencies and institutions to help prevent cyber-attacks by guaranteeing that all member-states possess the same information concerning malware, *modi operandi*, as well as past cyber-attacks that may have targeted other member-states. The use of cyber rapid-response teams, such as the NCIRC (NATO Computer Incident Response Capability) or its detachment RRT (Rapid Reaction Team), is also essential to aid member-states in the event of a cyber-attack. Training and best practice sharing is equally essential to guarantee that the Alliance members are able to reach roughly the same level; that is why the aforementioned NCI Academy, and its previous iterations, have been instrumental in this endeavour. Likewise, (cyber) exercises such as Cyber Coalition, Crossed Swords, NATO CMX, and Cyber Europe help put those best practices into action and solidify those skills and expertise. In conjunction, we saw the various partnerships that are in effect to also help NATO advance its cyber capabilities and abilities, such as partnerships with academia and industry/private sector who can help to greatly develop new technologies and offer insight into potentially new methods. Cooperation between governments, organizations, and tech companies to share best practices, intelligence, and coordinate responses can lead to more effective strategies, and involving civil society organizations, researchers, and academia in studying and addressing cyber issues can provide valuable insights, innovative solutions, and critical analysis. We also saw partnerships with NATO allied nations such as with Ukraine, through NATO's Trust Fund; Georgia, with

the SNGP (Substantial NATO-Georgia Package); and Japan, Ireland, Austria and others through the MN CD E&T (Multinational Cyber Defence Education and Training).

All these elements that have been pointed out here and throughout this thesis are essential when confronting the cyber threats NATO faces today, such as disinformation and misinformation, intellectual property theft and cyber espionage, critical infrastructure targeting, and false/no-flag attacks.

As we have seen, disinformation and misinformation can be used to great effect against nations where democracy and the rule of law prevail; with the aim of destabilising and polarizing it can be used to greatly alter or intensify public perception, opinions and reactions on certain issues, usually issues of a fracturing nature. Due to the nature of the internet in western democratic countries allowing for free speech, disinformation and misinformation have a higher degree of effect than countries such as China, Russia, Iran, or North Korea where internet traffic and usage is limited and (heavily) monitored, and the internet itself is domestically censored; A concrete illustration of this is the Great Firewall of China. In democratic nations, the internet operates without significant control or censorship, enabling the dissemination of disinformation or misinformation to reach a substantially larger audience compared to countries with more restrictive internet policies, such as those mentioned earlier. As Manuel Poêjo Torres states: "*The high proximity and exposure of democracies to cyberspace, places authoritarian powers in a privileged position, as they may exploit vulnerabilities […] at a very low cost and with high rewards.*"[261] We have seen in this thesis examples of how effective and dangerous this threat is to NATO, and the proportions it can take. Mitigating the spread of disinformation and misinformation on the internet is a complex challenge. First and foremost, member-states' governments could play a role in developing and

[261] Manuel Poêjo Torres, William Hasselberger, and Francisco Proença Garcia, "The Atlantic Posture and the 'Cybrid' Threats of Tomorrow," essay, in *O PODER AUTORITÁRIO E O DESAFIO PARA AS DEMOCRACIAS LIBERAIS* (Óbidos, Portugal: Alêtheia Editores, 2022), 130–69, 146-7.

implementing regulations and policies to address issues such as false political advertising, election interference, and online manipulation. Governments could also collaborate between civil society and companies to help promote and strengthen digital and media literacy as well as responsible online behaviour and sharing, both in the workplace and in schools to educate individuals about critical thinking, fact-checking, and responsible information consumption so they can distinguish between credible journalism and unreliable sources and understanding the methods and motives behind disinformation campaigns. Combating the spread of disinformation and misinformation requires a multifaceted approach involving various stakeholders, emphasizing education, technology, policy, and collaboration to reduce its influence and promote a more informed and resilient online ecosystem.

Intellectual property theft and cyber espionage in general are cyber threats that can be quite damaging – both economically and defence-wise – to NATO, and in particular, to member-states with a high degree of economic activity and large manufacturing companies, which can manifest in economic losses and strained international relations. The theft of defence-related intellectual property, whether it concerns cyberspace or not, can potentially have long-term and indirect repercussions on NATO, particularly in terms of its impact on defence systems. When sensitive intellectual property, specifically related to defence systems, is stolen, it jeopardizes the security, integrity, and operational effectiveness of NATO's defence infrastructure, which can undermine technological advancements, compromise critical military capabilities, and weaken NATO's ability to deter potential threats as well as potentially hindering its ability to effectively respond to emerging threats. The loss of intellectual property also poses a risk of proliferation, as stolen knowledge and technology can be exploited by adversaries or hostile actors to enhance their own military capabilities, as we have previously seen. Potential approaches to address these challenges include employing data obfuscation techniques to render data unintelligible or obscure as well as employing robust network security

protocols, encryption, access controls, and regular security audits, updates and patching; encouraging private companies to invest in robust cybersecurity measures through the implementation of Multi-Factor Authentication (MFA) and measures to secure supply chains and verify the integrity of hardware, software, and components used in critical systems as well as employee education and awareness concerning phishing attacks, social engineering techniques, and the importance of following security best practices; and developing intrusion detection systems capable of identifying abnormal network traffic and recognizing distinct patterns associated with known malicious actors. Fostering collaboration through public-private partnerships between government agencies, private sector entities, and international partners to share threat intelligence, tactics, and best practices, as well as establishing channels for timely and confidential information exchange can enhance detection and response capabilities. Additionally, enacting and enforcing strong legal frameworks that protect intellectual property rights and deter cyber espionage, including legislation that criminalizes intellectual property theft and provides adequate penalties for offenders should also be taken into account. Through the implementation of these solutions, NATO and its member-states can hope to enhance their ability to safeguard intellectual property, discourage cyber espionage, and foster a secure and resilient digital environment.

When it comes to CIS or CIP (Critical Infrastructure Security/Protection), in other words, the targeting of critical infrastructure, we have seen a substantial increase in quantity of attacks directed at these infrastructures, and likewise, an increase in complexity in these attacks and the tools used to carry them out. The repercussions of a cyber-attack on critical infrastructure exhibit considerable variability. Although such attacks typically avoid human casualties, they have the potential to disrupt vital services. This encompasses telecommunications, internet connectivity, and network outages that can significantly impact public sector operations. However, when control systems of crucial facilities like chemical

plants are targeted, the extent of damage inflicted can be far more severe, potentially affecting a wide geographical area. Consequences of such attacks can span from temporary inconveniences to deliberate acts of sabotage, intended to cause substantial harm and even result in explosions within industrial facilities, reverberating across domains critical to public health, national security, and the overall economy. One specific area of concern is the national power grid, which serves both public and private sectors. An attack on a strategic point within this infrastructure can trigger simultaneous shutdowns, impacting not only general electricity supply but also crucial sectors like hospitals and military bases. The intentional targeting of the power grid serves as an effective means to undermine a nation's military capabilities. This is due to the existence of numerous vulnerabilities and the complex network of interdependencies among critical infrastructures, amplifying the repercussions of an attack on any single infrastructure and magnifying the subsequent consequences for those reliant upon them. Our contemporary society, marked by a high degree of industrialization and reliance on complex infrastructural systems, exhibits a heightened vulnerability to disruptions within these intricate networks. The aftermath of a disruptive incident can yield an impact that far exceeds its magnitude, disproportionally affecting various facets of our interconnected world. Regarding the resolution of this problem, numerous approaches mentioned earlier can be equally employed here to address the matter at hand, such as strengthening cybersecurity measures, implementing best practices, regular training and awareness programs, and so forth. Likewise, we have seen that, recognizing the inherent interconnectivity of these systems, global adoption of methodologies in harmony with international standards is essential to effectively tackle the multifaceted challenges and mitigate the vulnerabilities posed by malware the likes of Stuxnet and its subsequent iterations.

Adding to this already complex and intricate array of problems, the landscape is further complicated by the presence of false-flag and no-flag attacks. It becomes evident, as we have

seen, that false-flag attacks and no-flag attacks do not inherently constitute distinct categories of cyber threats, but they are tactics employed to accomplish objectives that contribute to an already complicated issue. The attribution process, while not impossible, will be greatly hindered in the face of such attacks, and consequently, the repercussions and potential retaliatory actions may experience substantial delays or can even be avoided altogether. As such, developing and refining attribution techniques will make it harder for attackers to hide behind false-flag and/or no-flag tactics. Likewise, investing in the development of robust cyber threat intelligence capabilities to identify and analyse *modi operandi*, tactics, methods, and cyber tools, will facilitate the identification and attribution of future attacks of this nature.

To finalize, cyberspace has emerged as a domain of conflict, on par with the domains of air, land, sea, and space. One could argue that this particular domain holds greater importance, surpassing the other four, as it serves as the nexus that interconnects the remaining domains to one another. It is something that cannot, under any circumstance, be undervalued or belittled in today's increasingly interconnected world; doing so may entail even graver consequences. This is because many armed forces today depend on cyberspace to conduct their military operations; this is doubly so when it comes to NATO, where joint operations and military cooperation and interdependence rely greatly on a nexus for coordination and synchronization. Just as an air force safeguards airspace, an army operates on land to defend its borders, and a navy patrols territorial waters, so too must cyberspace receive an equivalent level of protection and attention. This is an essential element, as cyberspace represents a domain of sovereignty where each nation must assert its autonomy, particularly in the realm of defence, to maintain its sovereign status.[262] Therefore, to safeguard each Ally's national security, it becomes imperative to establish secure systems and communication infrastructures

[262] António Miguel Neves Almeida and Paulo Viegas Nunes, Interview: Brigadier General Paulo Viegas Nunes, personal, January 13, 2023. Refer to Appendix I, p. 151.

within cyberspace. The absence of a secure and reliable cyberspace capacity would render traditional armed forces ill-equipped to effectively counter an evolving array of threats.

In the face of this reality, cyberspace planning becomes a priority. However, unlike air, land, sea, and space, where environmental factors will not alter drastically in a short period of time, cyberspace is a rapidly changing environment, which makes planning a far more complex task; plans and entire strategies can become ineffective, or even obsolete, from one day to the next, so it becomes evident that the conventional planning methods employed in analogous domains are not effective when dealing with the digital characteristics of cyberspace. It is important to note that navigating the ever-changing landscape of cyberspace, while upholding technological superiority, can present formidable challenges without compromising or undermining core political values and ideals. To put it succinctly, democracies, including international organizations composed of democratic nations, encounter a distinct sluggishness, which we have explored earlier in this thesis. In contrast, autocratic nations do not experience this particular constraint. This gives autocratic nations an advantage we do not possess in terms of response times and their own cyberspace security and may weaken democracies due to its slow adaptability rate. We, however, should not be tempted to adopt these very methods and policies at the expense of our fundamental values as liberal democracies, even if we inadvertently find ourselves inclined to do so. Manuel Poêjo Torres states quite succinctly that "*[u]nknowingly, democracies may adopt policies, strategies, and procedures archetypal of autocracies and authoritarian powers, ultimately undermining their own core values.*"[263] As stated before, this is a risk that we must be acutely aware of when dealing with cyberspace planning, as there is a possibility of inadvertently adopting such policies without conscious realization.

[263] Manuel Poêjo Torres, William Hasselberger, and Francisco Proença Garcia, "The Atlantic Posture and the 'Cybrid' Threats of Tomorrow," essay, in *O PODER AUTORITÁRIO E O DESAFIO PARA AS DEMOCRACIAS LIBERAIS* (Óbidos, Portugal: Alêtheia Editores, 2022), 130–69, 149.

Lord Hastings Ismay, former NATO Secretary General, once coined the expression *Pax Atlantica*, which translates to Atlantic Peace, similar to the well-known historical period of prolonged peace within the Roman Empire, *Pax Romana*. To preserve this peace created by NATO means being ahead technologically, ensuring comprehensive mapping and extensive study of emerging disruptive technologies and tactics, as well as equipping the Alliance's cyberspace security capabilities and defence agencies – be they cyber-related or not – with the necessary expertise to navigate this new domain with a reasonable level of confidence. As we have explored, partnerships are extremely important for NATO as they ensure heightened effectiveness in addressing cyber-threats and maintaining surveillance over the cyberspace domain. However, the most important partnership is with the European Union, as many members of NATO are also members of the EU. Both NATO and the EU should adopt synchronized and parallel defence strategies, reinforcing the military, as well as the civilian aspects with the necessary capabilities to effectively counter precision attacks targeting their core vulnerabilities. Doctrine, including its development, holds significant importance for the Alliance, and the trio comprising the NATO Defence College, the NATO School in Oberammergau, and the CCDCOE's Tallinn Manuals form NATO's cyberspace doctrine. It is crucial to continuously refine these resources to uphold and enhance NATO's superiority in the cyberspace domain.

We need to perceive cyberspace not as a separate domain but as an integral component that significantly influences the performance and success of forces operating across other domains, so therefore, special attention must be given to cyberspace, including the development of cyber capabilities, doctrine, and all other factors examined and explored throughout this thesis, and we must also be acutely aware that the security of individual member-states impacts the defence of the Alliance as a whole.

The Athenian admiral and archon Themistocles once stated that "*he who controls the sea controls everything.*"[264] This was uttered at a time when the seas were the network that connected peoples and civilizations across the known world, and, as history tells us, that remained an unquestionable truth until quite recently. From the time of Athenian naval supremacy to the Roman Republic and Empire, from the Islamic Caliphates to the supremacy of the Portuguese and British Empires, this maxim remained undeniable. Today, the variable has changed, but the fundamental principal remains no less relevant; today, cyberspace has taken the place of the sea as the network that connects the world; today, he who controls cyberspace, controls everything. Cyberspace has evolved today into the largest, most rapidly expanding, and intricately interconnected repository of human knowledge ever constructed. It serves as a vast network that intertwines countless facets of global economic activity, trade, and human existence, with the power to exert influence over the political landscape. Therefore, if NATO wishes to safeguard our way of life and the principles of freedom, liberty, democracy, equality, and the rule of law upon which our Western civilization is founded, then it is essential that superiority over cyberspace is guaranteed and maintained, just as it is on land, at sea, and in the air; and it must do so without compromising or betraying those very principles to which we hold so dearly.

[264] Marcus Tullius Cicero, "Letter to Atticus 10.8.4.," 68AD.

PAGE LEFT INTENTIONALLY BLANK

PAGE LEFT INTENTIONALLY BLANK

Bibliography

ALMEIDA, António Miguel Neves, and António Gameiro Marques. Interview: Rear-Admiral António Gameiro Marques. Personal, January 23, 2023.

ALMEIDA, António Miguel Neves, and Lino Santos. Interview: Coordinator Lino Santos. Personal, February 13, 2023.

ALMEIDA, António Miguel Neves, and Paulo Viegas Nunes. Interview: Brigadier General Paulo Viegas Nunes. Personal, January 13, 2023.

ANTONIUK, Daryna. "Ukraine Signs Agreement to Join NATO Cyber Defense Center." *The Record*, January 20, 2023. https://therecord.media/ukraine-signs-agreement-to-join-nato-cyber-defense-center.

BAJAK, Frank. "Cyberattacks Accompany Russian Military Assault on Ukraine." *Associated Press*, February 24, 2022. https://apnews.com/article/russia-ukraine-technology-business-europe-russia-9e9f9e9b52eaf53cf9d8ade0588b661b.

"Brussels Summit Communiqué." *NATO*, June 14, 2021. NATO. https://www.nato.int/cps/en/natohq/news_185000.htm.

"Brussels Summit Declaration." *NATO*, July 11, 2018. NATO. https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

BUNDESDRUCKEREI. "Tasks of Germany's Cybersecurity Institutions." Bundesdruckerei. Accessed November 16, 2022. https://www.bundesdruckerei.de/en/innovation-hub/name-cybersecurity#:~:text=In%202018%2C%20the%20German%20government,in%20the%20field%20of%20cybersecurity.

BUNDESREGIERUNG, ed. "The National Cyber Response Centre." Federal Office for Information Security, August 2, 2022. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum.html.

BUNDESWEHR. "The Cyber and Information Domain Service." Bundeswehr. Accessed November 15, 2022. https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service.

CABINET OFFICE, and HM Government, NATIONAL CYBER SECURITY STRATEGY 2016-2021 § (2016). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

"China: Declaration by the High Representative on Behalf of the European Union Urging Chinese Authorities to Take Action against Malicious Cyber Activities Undertaken from Its Territory." *European Council*, July 19, 2021. European Union.

https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/.

CHO, Sungbaek. “Enhancing Cybersecurity of Industrial Control Systems.” Essay. In *Enabling NATO’s Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)*, edited by USAWC Press, 355–85. Carlisle, PA: Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022.

CICERO, Marcus Tullius. “Letter to Atticus 10.8.4.,” 68AD.

CNCS. “Additional Recommendations.” Essay. In *National Cybersecurity Framework*, 144. CNCS, 2020. https://www.cncs.gov.pt/docs/qnrcs-web-eng.pdf.

CNCS. “C-Academy.” CNCS. Accessed February 24, 2023. https://www.cncs.gov.pt/pt/c-academy/.

COCOLAN, Miruna-Maria. Ms. *International Cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence* . Romania, 2018. https://www.cipre-expo.com/wp-content/uploads/2018/10/Cocolan%20M%20NATO-UKRAINE%20Trust%20Fund%20on%20Cyber%20Defence.pdf.

COLLINS, Stuart. “Cyber Attacks on Critical Infrastructure.” AGCS Global, June 2016. https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

COMCYBER, ed. “Les Missions et La Chaîne de Commandement Du Commandement de La Cyberdéfense.” Defense.gouv.fr. Accessed November 3, 2022. https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber.

“Cyber Defence Pledge.” *NATO*, July 8, 2016. NATO. https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

“CYBER EXERCISE PROVES READINESS TO RESPOND TO CYBER THREATS.” *PESCO*, May 28, 2021. European Union. https://www.pesco.europa.eu/wp-content/uploads/2021/05/PRESSSTATEMENT-CRRT.pdf.

DAVIS, Susan. *NATO IN THE CYBER AGE: STRENGTHENING SECURITY & DEFENCE, STABILISING DETERRENCE*. London, United Kingdom: NATO Parliamentary Assembly’s Science and Technology Committee (STC), 2019.

THE DEFENSE POST. “Ukraine Joins NATO Cyber-Defense Center.” *The Defense Post*, May 17, 2023. https://www.thedefensepost.com/2023/05/17/ukraine-joins-nato-cyber-defense/.

Department of Defense Dictionary of Military and Associated Terms (incorporating the NATO and IADB dictionaries), November 2021 ed. (Washington, D.C., United States of America: Joint Chiefs of Staff, 1987), s.v. “Cyberspace Defence.,”

DONN, Natasha. “Armed Forces Centre for Cyber Defence Suffers New Attack.” *Portugal Resident*, October 2, 2022. https://www.portugalresident.com/armed-forces-centre-for-cyber-defence-suffers-new-attack/.

DONN, Natasha. “Hundreds of NATO Documents Sent to Portugal Discovered for Sale on Dark Web.” *Portugal Resident*, September 8, 2022. https://www.portugalresident.com/hundreds-of-nato-documents-sent-to-portugal-discovered-for-sale-on-dark-web/.

EFTHYMIOPOULOS, Marios Panagiotis. “A Cyber-Security Framework for Development, Defense and Innovation at NATO.” *Journal of Innovation and Entrepreneurship* 8, no. 1 (2019). https://doi.org/10.1186/s13731-019-0105-z.

ENISA, ed. “NIS Directive.” European Union Agency for Cybersecurity, October 13, 2022. https://www.enisa.europa.eu/topics/nis-directive.

EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy § (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN.

GERRITS, André W.M. “Disinformation in International Relations: How Important Is It?” *Security and Human Rights* 29, no. 1–4 (2018): 3–23. https://doi.org/10.1163/18750230-02901007.

GOVERNO DE PORTUGAL, ed. “Estratégia Nacional de Segurança Do Ciberespaço.” Portugal Digital, June 20, 2022. https://portugaldigital.gov.pt/acelerar-a-transicao-digital-em-portugal/conhecer-as-estrategias-para-a-transicao-digital/estrategia-nacional-de-seguranca-do-ciberespaco/.

GRIEVE, Dominic, Intelligence and Security Committee of Parliament Annual Report 2016–2017 § (2017). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727949/ISC-Annual-Report-2016-17.pdf.

JONES, Jeffrey B. “Confronting China’s Efforts to Steal Defense Information.” Harvard Kennedy School Belfer Center for Science and International Affairs, May 2020. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.

KASPERSKY. “What Is Cyber Security?” www.kaspersky.com, May 16, 2022. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

KOVÁCS, László. “CYBER SECURITY POLICY AND STRATEGY IN THE EUROPEAN UNION AND NATO.” *REVISTA ACADEMIEI FORŢELOR TERESTRE* 1, no. 89 (2018): 16–24.

LIANG, Qiao, and Wang Xiangsui. *Unrestricted warfare*. Beijing: PLA Literature and Arts Publishing House Arts, 1999.

"Lisbon Summit Declaration." *NATO*, November 20, 2010. NATO. https://www.nato.int/cps/en/natolive/official_texts_68828.htm.

"Madrid Summit Declaration." *NATO*, June 29, 2022. NATO. https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

MARSHALL, Hannah, and Alena Drieschova. "Post-Truth Politics in the UK's Brexit Referendum." *New Perspectives* 26, no. 3 (2018): 89–105. https://doi.org/10.1177/2336825x1802600305.

MARTIN, Alexander. "Japan Formally Joins NATO Cyber Cooperation Center." *The Record*, November 4, 2022. https://therecord.media/japan-formally-joins-nato-cyber-cooperation-center.

MINISTERIO DE DEFENSA, ed. *Spanish Approach to Cybersecurity*, June 2019. https://www.ccn.cni.es/index.php/en/docman/documentos-publicos/23-decalogue-spanish-approach-to-cybersecurity-2018/file.

MINISTRY OF DEFENCE, and Bundesregierung, WHITE PAPER 2016 ON GERMAN SECURITY POLICY AND THE FUTURE OF THE BUNDESWEHR § (2016). https://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf.

MUELLER, Robert S., Report on the investigation into Russian interference in the 2016 presidential election: Submitted pursuant to 28 C.F.R. §600.8(c) § (2019). https://www.justice.gov/archives/sco/file/1373816/download.

NATIONAL CYBER SECURITY CENTRE, GCHQ § (2019). https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims.

NATO, ed. "The Substantial NATO-Georgia Package." NATO, February 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/2/pdf/Cyber-Defence-georgia.pdf.

NATO, ed. "UKRAINE Cyber Defence - NATO Trust Fund." NATO, June 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf.

NATO, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization § (2010). https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

NATO-CR14, ed. "Cyber Ranges." CR14. Accessed March 15, 2023. https://www.cr14.ee/ranges#nato-cyber-range.

NATO-MNCDET, ed. "Participants: MNCDET-NATO." MN CD E&T. Accessed March 17, 2023. https://mncdet.wixsite.com/mncdet-nato/participants.

NATO. “Cyber Defence.” NATO, July 14, 2022. https://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO. *Defending the Networks - The NATO Policy on Cyber Defence*. NATO Graphics & Printing, 2011.

NATO. “NATO Communications and Information Agency (NCI Agency).” NATO, May 20, 2019. https://www.nato.int/cps/en/natolive/topics_69332.htm.

NATO. “NATO Defence Planning Process.” NATO, July 9, 2021. https://www.nato.int/cps/en/natohq/topics_49202.htm.

NCI Agency, ed. “NCI Agency: About the NCI Academy.” NCI Agency | About the NCI Academy. Accessed January 12, 2023. https://www.ncia.nato.int/what-we-do/nci-academy/about-the-nci-academy.html.

NCSI. “France.” National Cyber Security Index. Accessed September 3, 2022. https://ncsi.ega.ee/country/fr/.

NCSI. “Germany.” National Cyber Security Index. Accessed September 3, 2022. https://ncsi.ega.ee/country/de/.

NCSI. “Portugal.” National Cyber Security Index. Accessed September 3, 2022. https://ncsi.ega.ee/country/pt/.

NCSI. “Spain.” National Cyber Security Index. Accessed September 3, 2022. https://ncsi.ega.ee/country/es/.

NCSI. “United Kingdom.” National Cyber Security Index. Accessed September 3, 2022. https://ncsi.ega.ee/country/gb/.

NCSI. “United States.” National Cyber Security Index. Accessed September 3, 2022. https://ncsi.ega.ee/country/us/.

PERNIK, Piret, Jesse Wojtkowiak, and Alexander Verschoor-Kirss . “National Cyber Security Organisation: UNITED STATES.” CCDCOE, 2016. https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf.

PIHELGAS, Mauno, ed. “Mitigating Risks Arising from False-Flag and No-Flag Cyber Attacks.” CCDCOE, March 31, 2015. https://ccdcoe.org/uploads/2018/10/False-flag-and-no-flag-20052015.pdf.

PITEIRA NATÁRIO, Rui Manuel, and Paulo Fernando Viegas Nunes. “RISCO SOCIAL NO CIBERESPAÇO. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS.” *Revista Militar*, no. 2547 (April 2014). https://www.revistamilitar.pt/artigo/913.

PORTUGUESE REPUBLIC. “ANNEX - National Strategy for Cyberspace Security 2019-2023.” Essay. In *Portuguese Official Journal* 108, Vol. 108. Series 1. Imprensa Nacional, 2019.

"Prague Summit 2002 - Selected Documents and Statements." *NATO*, 2002. NATO. https://www.nato.int/docu/0211prague/speeches-e.pdf.

REUTERS. "Computer Virus Infects Spain's Defence Ministry: Report." *WION*, March 26, 2019. https://www.wionews.com/world/computer-virus-infects-spains-defence-ministry-report-205782.

"Riga Summit Declaration." *NATO*, November 29, 2006. NATO. https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en.

"Russian Project Lakhta Member Charged with Wire Fraud Conspiracy." *Department of Justice*, September 10, 2020. https://www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy. Press Release Number: 20-902

SABATINO, Ester, and Alessandro Marrone. "Cyber Defence in NATO Countries: Comparing Models." Academia, February 2021. https://www.academia.edu/45124767/Cyber_Defence_in_NATO_Countries_Comparing_Models.

SCADA International, ed. "Learn All about SCADA Systems: What Is SCADA?: Scadapedia." SCADA International, April 20, 2023. https://scada-international.com/what-is-scada/?utm_medium=cpc&utm_source=google.com&utm_campaign=scada-explained&gad=1&gclid=CjwKCAjwpayjBhAnEiwA-7ena7ZeocaHWLY53gJfOGz5AqmJXX8lfJz7yD9E7-kHVUTN09svXBmOtBoCjfkQAvD_BwE.

SCHATZ, Daniel, Rabih Bashroush, and Julie Wall. "Towards a More Representative Definition of Cyber Security." *The Journal of Digital Forensics, Security and Law* 12, no. 2 (June 30, 2017): 55–57. https://doi.org/10.15394/jdfsl.2017.1476.

SGDSN, Revue stratégique de cyberdéfense § (2018). https://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf.

SGDSN, Strategic review of cyber defence § (2018). https://www.sgdsn.gouv.fr/files/files/Publications/revue-cyber-resume-in-english.pdf.

SKOPIK, Florian, and Timea Pahi. "Under False Flag: Using Technical Artifacts for Cyber Attack Attribution." *SpringerOpen* 3, no. 8 (March 20, 2020). https://doi.org/https://doi.org/10.1186/s42400-020-00048-4.

"Statement by the North Atlantic Council Concerning Malicious Cyber Activities." *NATO*, June 3, 2020. NATO. https://www.nato.int/cps/en/natohq/official_texts_176136.htm.

"Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise." *NATO*, July 19, 2021. NATO. https://www.nato.int/cps/en/natohq/news_185863.htm.

STOUFFER, Clare. “10 Types of Malware + How to Prevent Malware from the Start.” Norton, August 27, 2021. https://us.norton.com/blog/malware/types-of-malware.

TORRES, Manuel Poêjo, William Hasselberger, and Francisco Proença Garcia. “The Atlantic Posture and the ‘Cybrid’ Threats of Tomorrow.” Essay. In *O PODER AUTORITÁRIO E O DESAFIO PARA AS DEMOCRACIAS LIBERAIS*, 130–69. Óbidos, Portugal: Alêtheia Editores, 2022.

UNITED STATES CYBER COMMAND, Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command § (2018). https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

USCYBERCOM, ed. “Our Service Cyber Partners.” U.S. Cyber Command. Accessed September 27, 2022. https://www.cybercom.mil/Components/.

VASS, Sandor. “Panel 2 - Cyber Resilience & Preparedness: Harmonizing Requirements to Delivering Operational Capabilities: Cyberspace Operations Centre - A Capability User Perspective.” Academia Militar, 2018. https://academiamilitar.pt/images/site_images/5th_NATO_Cyber_Defence/8_Brigadier_General_HUN_Army_Sandor_VASS_Director_Cyberspace_Operations_Centre_ACO_-_CyOC.pdf.

“Wales Summit Declaration.” *NATO*, September 5, 2014. NATO. https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

WARD, Alex. “4 Main Takeaways from New Reports on Russia’s 2016 Election Interference.” *Vox*, December 17, 2018. https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram.

“Warsaw Summit Communiqué.” *NATO*, July 9, 2016. NATO. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

WEINER, Rachel. “Russian National Accused of Fraud Conspiracy Aimed at Political Interference.” *Washington Post*, September 10, 2020. https://www.washingtonpost.com/local/legal-issues/russian-national-accused-of-fraud-conspiracy-as-part-of-election-interference/2020/09/10/abfda006-f370-11ea-bc45-e5d48ab44b9f_story.html.

THE WHITE HOUSE, National Cybersecurity Strategy § (2023). https://www.cybercom.mil/Portals/56/Documents/Mission%20and%20Vision/National-Cybersecurity-Strategy-2023.pdf.

ŠTRUCL, Damjan. “Comparative Study on the Cyber Defence of NATO Member States.” NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2021. https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf.

PAGE LEFT INTENTIONALLY BLANK

Appendix

Appendix I – Interview Transcript: Brigadier General Paulo Viegas Nunes

Appendix I.a – English Translation

[START]

Paulo Viegas Nunes: Talking solely about cybersecurity in the context of NATO in Portugal's alliance logic is limiting. It's limiting because, on the other hand, the European Union is initiating a similar effort, and there is another integrating element of the strategic vision of the European Union and NATO, which is usually consolidated in joint declarations at summits, including the latest summit, focusing on cooperation aspects. Why am I mentioning this? Because Portugal, being a member of both international organizations, cannot solely focus its strategic orientation and policy on the field of cybersecurity and cyber defence from one side. It has to maintain an equidistant position between the two and has every advantage to ensure that its actions are perfectly aligned with the defined objectives. Moreover, this is not a unique case. We have over 20 countries in the same situation. Until recently, it was 23, now it's 22 because the United Kingdom left the European Union. But this is to emphasize that a master's dissertation would benefit from this broad perspective, considering the framework of alliances and the external vision of national foreign policy. Therefore, in practice, what we are discussing is cybersecurity within the framework of national strategic vision and subsequently the international framework of security and defence, which connects with the later topic. Thus, Portugal's security and defence are designed in terms of vision around these two pillars within the scope of security and defence. That's what I have been doing.

António Neves Almeida: I have some references in my thesis about the European Union, but I need to focus more on the NATO part and the national strategies of some countries regarding how they have adapted, in other words, how they have formulated their cyber strategies. Because some countries have a more offensive strategy in their cybersecurity, like the United Kingdom and the United States, while others have a more defensive approach, like Germany, Spain, etc. Sometimes it's due to legislative and political reasons, as how the powers are divided in those countries. And sometimes it's simply because the country itself doesn't have the means to have a more active security approach.

P.V.N. It's not about the nature of cyber defence; it's about the vocation, the vision of the role of cyber defence. Offensive capability is crucial for a good

defence. Without that deterrent capability and ensuring defence, there is no possible defence.

A.N.A. The initial questions are quite simple, basic ones, such as how do you see the state of the art of cybersecurity and cyber defence in general? How do you see it in national terms? And how do you see it in terms of NATO?

P.V.N. In terms of the maturity of NATO's strategic vision, it surpasses ours. Essentially, for one reason. Our framework is a bit delayed in terms of construction. As you may know, the national cyber defence strategy was only approved on November 2nd, so it is very recent when the strategic vision and underlying logic for capability development in other countries have been in place for a long time. In some cases, even for a decade or more. Countries like the United States established their cyber command in 2009 and had it fully operational by 2011. When we compare this to our current state, already in 2023, with the strategy approved in November 2022, it's challenging to consider our maturity level as equivalent, isn't it? There is a significant dissemination gap. The United States is a prominent partner within NATO, and their strategic and operational logic aligns closely with the security and defence policies of the United States. As a global actor projecting power on a global scale, the United States has a strong defence value and, as such, needs robust capabilities in specific areas. Nowadays, cyberspace is a prioritized area for power projection due to its pervasive nature and the effects it produces in these domains. In practice, what we are discussing is an instrument of hybrid warfare, where the multi-agency approach resulting from the cross-cutting nature of cyberspace itself is a significant challenge. Perhaps the biggest challenge for humanity. Therefore, in terms of national maturity, I believe we are somewhat behind. On the other hand, within the organizational aspect, the Armed Forces General Staff, within its latest parliamentary decree resulting from the Organic Law on Armed Forces (LOBOFRA), which was revised and approved, includes a command for cyber defence operations at various levels. However, in my opinion, the organization is not optimal yet because it is understaffed, and from a command relationship perspective, it is not in the right place. If we apply the existing doctrine, both at the American and NATO levels, all operational domains have a structured command and control around that domain. It means that, in practice, what I am saying is that the command of cyberspace should be similar to the command of land forces, the air force, or the navy. There should be a cyberspace command following the same pattern. And this cyberspace command should be directly linked to the joint operations command to coordinate the required utilization across various operational domains, even in a multidomain logic for implementing the projection of military force. Another area where I believe we need to grow at the national level is the use of military components. Currently, we have a cybersecurity structure that is more or less consolidated, with the National Cybersecurity Centre at its core, and then an ad hoc architecture called G4, which convenes in case of a disruptive large-scale operation. The G4 is composed of whom? It includes the cybersecurity structure, personalized by the National Cybersecurity Centre, the law enforcement or criminal investigation part with the Judicial Police and the C3T

unit, which is the Technological Crime Combat Unit of the Judicial Police, the CIS (Information and Security System), and the Armed Forces' Cyber Defence Centre, which has not yet established the Cyber Defence Command and is still in the implementation phase. What does this bring? It brings coordination at the cybersecurity level. If there is an intervention in cyber defence, in other words, if the effect is destructive or disruptive on a large scale, the coordination of this national response shifts from the security domain to the defence domain. However, there is no structure in place to act in that scenario. We can say that G4 serves both cybersecurity and cyber defence. It's true, but from a political standpoint, the oversight is completely different. In the specific case, the National Cybersecurity Centre reports directly to the Council of Ministers. In the case of cyber defence, it falls under the Ministry of Defence, naturally through the Armed Forces General Staff. There is no inter-ministerial coordination within the Armed Forces General Staff, as the British term it, an "all of state" response that is aggregated, multi-agency, multidimensional, and multisectoral. This requires a national decision at the highest level, which is the presidency of the Council of Ministers. And the only entity with access to the Presidency of the Council of Ministers is the National Cybersecurity Centre. It means that the national response is predominantly channelled towards the cybersecurity domain. If there was a need to activate the cyber defence capability, what we would need is a pre-approved operations plan, coordinated among all the ministries.

A.N.A. And we don't have that.

P.V.N. No, we don't. We also don't have the capacity with the current structure to ensure that it is done promptly. And that is the part that weakens the coordination of cyber defence within a framework that requires a cross-cutting approach. Therefore, my logic is based on the fact, and I have described it, I have published a vision in that direction, that we need a National Council for Cyberspace Defence. Currently, we have a National Council for Cyberspace Security, where various entities are involved in handling a crisis related to cybersecurity. But if we have a crisis in the realm of cyber defence, we need to convene the various entities under the presidency or coordination of the Ministry of Defence. It cannot be the same approach we have for cybersecurity. Therefore, it is this coordination that is lacking in the construction of the framework.

A.N.A. And do you think we are still far from reaching that point?

P.V.N. Not too far. We are following the path, aren't we? At the moment, and I believe we should be somewhat satisfied with this progress, what we are doing is constructing the framework. We have developed or identified the cyber defence strategy, which we didn't have before but now we do. There is an implementation plan for the cyber defence strategy, and it is underway. Previously, there were only guiding principles for the cyber defence strategy, but now we have a serious plan, the ENCFAC, which is the General Staff of the

Armed Forces, responsible for its implementation. What is lacking now is the creation of this body, which is a political level entity. It is a political-level organization, not a military-level organization. It has to be a defence-level entity, not one belonging to the Armed Forces. Interestingly, the model I have developed is a pyramid model. And this pyramid model helps to explain this. What do we have in the pyramid model? We have two pyramids, one for cybersecurity and another for cyber defence, at the national level, which are connected at various levels. And there it becomes clear what I am saying in terms of connection and coordination because technical coordination, operational coordination, strategic coordination, and political coordination all need to exist. If we view this as a pyramid model with layers, it becomes clearer. And then we need to actually establish the political law for cyber defence, which doesn't exist yet. That is the missing law. What does this lead to? It leads to the fact that whenever the state needs to discuss matters related to cyber defence, whether at the NATO level or the European Union level, politically, it falls under the realm of cybersecurity. In other words, we need to have the right interlocutors within the international component. The pyramid model is completed with two other pyramids that surround these national pyramids and mobilize the state's vision for the two dimensions. On the political and cybersecurity fronts, our primary and central partner is the European Union. Therefore, there is a pyramid for cybersecurity within the European Union. In the military domain, our pyramid is the NATO pyramid. And there is another pyramid there. This means that at the NATO level, when discussing cyber defence, particularly at the NATO Cyber Defence Committee (CDC), if we need to take official positions, it cannot be the cybersecurity sector representing the country in that domain. It has to be someone from the political level, indeed, but in the field of cyber defence. This part is missing. The pyramid model makes this very clear. I found this model explained and mapped in the book I wrote during my recent senior officer promotion course, highlighting the need for the development of a military cyber defence strategy. It is something distinct from the national cyber defence strategy.

A.N.A. What is the name of that book?

P.V.N. It is at MUI, at the Military University Institute, and it was my final research project for the promotion course to General Officer, part of the Ares 28 collection, I believe.

A.N.A. That actually answered the next two questions as well. One of the next questions was what was missing in terms of national security and defence? And then the other question was what do you think is still lacking in the NATO context? Why do you think NATO needs to do more? Is NATO capable of defending itself against other powers, or is there still a long way to go…?

P.V.N. NATO has a constructive ambiguity. What is constructive ambiguity? It is the use of Article 5 in the event of a cyber-attack. The biggest problem with cyber-attacks is that they are constant. There is no peace, no war. They can

escalate immediately from one moment to another, and if there is no mechanism for reserve or control from the perspective of crisis evolution, it forces the invocation of Article 5, basically. And NATO cannot do that, otherwise it would be constantly declaring war. This is something that is not acceptable from a strategic point of view. NATO has a defensive strategy, openly adopting a defensive strategy. It has been changing with the conflict in Ukraine, so there have been certain adjustments. But it means that it does not renounce the use of offensive means. It has a strategy that involves the concept of Strategic Production of Effects. Basically, the concept is the production of effects by countries in favour of NATO. Countries provide NATO with their offensive capabilities, and if NATO needs to act offensively with cyber capabilities, it does not act as NATO itself, but requests a country with the capabilities to act as the "NATO of NATO." So, it's a bit different from our traditional view of using military power, but that's effectively what happens. So, what is still missing to build within NATO? Firstly, a clear understanding of the operational domain of cyberspace with strategic command for cyberspace. NATO has strategic commands, divided into strategic commands that usually specialize in air and specific land capabilities, etc. What is missing is a strategic command for the Cyber Defence Initiative. Currently, in the area of cyber defence, there is the CIOC, which is the Operational Cyber Command within the CIS command or department. It is the same person who serves as the dual link, but it is not a command. It is an operational plan in itself. This will naturally progress because the disruptive and destructive capacity of this domain is growing, and there will be more and more integrated planning. However, it needs to be strengthened, not only at the individual level of each country, which is already happening, but also at the level of collective defence, specifically within NATO.

A.N.A. One could even say that this is already happening, to some extent, through the training centre in Estonia, through the NCI Academy.

P.V.N. It's not the same thing. What we are discussing is an operational command. What you are referring to is a centre of excellence that provides training, doctrine, etc. In the specific case of the NCI Academy in Oeiras, what we are talking about is a school that also provides training in that area. It's not a pure "cyber" school. I don't know if you have this information, but I was the first commander of that school here, and I was involved in the process of introducing a cyber curriculum at the time. In fact, it stemmed from a project that Portugal led, and I was also the project manager for that. It was a project called the Multinational Cyber Defence Education and Training, which was a NATO Smart Defence project that coincidentally developed a curriculum that was also adopted by the European Union. Portugal also led the Cyber Defence Discipline, specifically within the European Union's EU Military Training Group (EUMTG). Portugal led both parts. We led the Multinational Cyber Defence Education and Training and the Cyber Defence Discipline within the European Union. We established an extension of this group here in Portugal. At a certain point, we aligned the work plan and the curriculum, so any initiatives produced in each of these three domains automatically projected to the others.

We created a very interesting cooperation system and organized several Smart Defence project seminars in the cyber area at the Lisbon Military Academy in Amadora, specifically within NATO, in collaboration with the European Union and other partners. But having a centre of excellence, a school, and an operational core are not the same approach. They are different things.

A.N.A. No, what I meant by that was that... Although there isn't something centralized, there is already some form of it... In other words, there is no... We have a country training itself, developing its own capabilities. And in this way, we could eventually say that NATO is helping countries train each other, helping to train each other through these centres of excellence.

P.V.N. The concept is collective defence. In order to have collective defence, to have collaboration, there needs to be common doctrine and training, otherwise people cannot act together. That's what we're talking about.

A.N.A. I had another question here. Essentially, it was whether the current situation of each country developing itself, does it harm NATO? Does it undermine NATO's ability to defend itself? Or would it be better for NATO to have a central structure, a unified policy, a unified strategy for all countries?

P.V.N. It has to be. In fact, the cyberspace domain is an area of sovereignty, and we must not forget that. Each country has to be sovereign, and to be sovereign, it must be autonomous in the defence component of that domain. It is an inalienable responsibility. It's not the kind of responsibility that can be delegated to third parties. It is essential that each country feels this. But just as they understand the dimension of collective defence, which is a cooperative defence, it is not the defence of an isolated country. It's a team sport, as the English say. Naturally, all of this requires joint action. That's why NATO has exercise plans and doctrine. Doctrine consists of principles of action that are shared by all. Therefore, if we have the notion that we have to work together in the same way, train in the way we work, we will create synergies. The difference here is that each country does its own thing, each develops its own exercises, and there is no guarantee that things will converge afterward. But NATO has to do it if it wants to act with unity of effort and unity of command, which is the fundamental principle.

A.N.A. Do you consider that Portugal is still at risk of being a mere executor of strategies dictated by leading nations or organizations in this field?

P.V.N. I believe that Portugal has the duty and rightful expectations to have its autonomy and its own assertion in this domain. In fact, in a conversation with a friend from the United Kingdom who was involved in developing national cyber defence capabilities, I asked him, "So how did you manage to shift the mindset or 'mindshift' in this case to improve these types of capabilities and create

equipment for development?" He gave an answer that, after thinking about it, I considered to make perfect sense. They explained the need for such a capability based on a macroeconomic analysis. In other words, the UK's economy is projected to be 70% digital by 2030. This means that if the digital environment or ecosystem is attacked and, as a result, unavailable, the country will collapse from an economic perspective. Added to this are concerns about critical infrastructure and the concept of resilience, which gained significant attention during the pandemic process. The COVID-19 pandemic brought significant challenges to various states and international organizations in terms of survival in the digital realm and transformation. It wasn't just about survival; it was about transformation. Therefore, the focus shifted from discussing security alone to discussing security and resilience. Resilience is a key word in this context. And that's why the cyber component is crucial; it is a necessary condition and sometimes not sufficient, but it is a necessary condition for the digital resilience of a state. Portugal clearly has a very strong level of ambition in terms of its vision for digital transformation and transition. To architect a strategy of assertion in this domain, it must include strong security and defence measures because otherwise it becomes vulnerable, it becomes fragile. Take, for example, our debit cards. We hardly carry physical cash in our wallets anymore; the card has become the virtual wallet. But if there is no way to make a payment, the economy stops. It stagnates. There are no commercial transactions, and even the few who still have physical cash lose its value within seconds or minutes of the interruption of digital economic flows. Then we have the control systems for electricity, gas, water, and traffic, including air traffic. And these are just a few examples. Communications themselves can be targeted by cyber-attacks, and our country has been the target of several cyber-attacks in recent months. Last year was particularly fertile, but this year we have already seen a growing trend that is not going to diminish. All of this needs protection, it needs defence to be resilient. Therefore, Portugal cannot neglect this component in any way and must have a very consistent plan to achieve resilience. Human resources are very limited and naturally require an extensive training period.

A.N.A. I'll also take this opportunity to ask you another question that is specifically for you. In 2014, you wrote an article in the military magazine with Lieutenant Colonel Piteira Natário, where you discussed critical infrastructure. I would like to ask if, nine years later, you believe that these critical infrastructures are better safeguarded today than they were in the past? And if so, if the current level of protection is sufficient or if there is still more to be done? Naturally, there is always more to do, but do you consider that there is still much more to be done?

P.V.N. In June of last year, I wrote another article for EuroDefence that was published in the national edition and later in the international edition with engineer Paulo Moniz from the EDP group. What I believe has now emerged is a better understanding of the vulnerabilities and interconnections of various critical infrastructures. Because there are indeed very different situations among them, which is incredible. The European Union has called for a plan in this regard and is introducing specific legislation to ensure minimum levels of

resilience, not only for critical infrastructures but also for what it designates as essential services. These can include not only physical infrastructures but also essential services such as social security, the IT system, tax services, property databases, justice ministry databases, and anything that has intangible value but is essential for society to function. On the NATO side, there has also been a consistent effort in this domain. NATO refers to them as the foundational pillars of resilience. A joint declaration by NATO and the European Union was made at the Warsaw Summit in 2016, defining several sectors where collaboration between the military component and civil preparedness, with the support of the armed forces, is necessary to ensure state resilience. This has been elevated to the NATO level, meaning it's not just about state resilience but also about the resilience of the NATO structure itself. Why am I mentioning this? Because it parallels the case of the European Union. The EU has also taken similar steps, imposing recommendations on member states, aiming to achieve common resilience. For example, in the common electricity and gas markets, there is talk of coordination and joint action among various entities working in civil protection within the European Union. There is an awareness that emergencies and protection are necessary beyond borders, not just within them, and given the interconnectedness of networks, from energy to communications, etc., protection cannot be limited to internal perimeter protection; it must be an aggregated and ecosystem-wide approach. This changes people's mindset, and I believe we have evolved to some extent in terms of maturity in this regard.

A.N.A. Do you consider that cyberspace and the dependence on cyberspace are highly important for NATO today, including its day-to-day operations and military operations, where there is an increasing reliance on cyberspace? Do you believe that this dependence has grown? Is it now even more crucial and in need of appropriate protection?

P.V.N. Yes, I believe it is a cross-cutting issue, not just for NATO but for all institutions in all countries. The tendency grows as the connection to networks increases because these types of threats operate through networks, and it is the network that somehow maximizes and promotes the diffusion of such threats. Beyond the infrastructural growth, we have another type of growth that is becoming increasingly visible and evolving on an unprecedented scale. This growth relates to the cognitive pyramid. We are transitioning from purely infrastructural attacks, which are attacks at the level of bits and bytes, information flows, to attacks that target the structure of information itself, such as syntax, the way characters and information are structured. This is related to the realm of information warfare and disinformation. Moreover, there is another component that builds upon this, which is the cognitive aspect. We are entering a network logic where we no longer focus solely on the syntax, the characters, and how information is presented, but rather on the semantics, the meaning of information and how we interact at that level. In practice, this means shifting from searching for character occurrences to searching for ideas. It means that when we promote dissemination and manipulate a certain environment supported by cyberspace, we manipulate beliefs and perceptions instead of manipulating information structures. And this indeed makes all the difference.

A.N.A. How do you assess the importance of cyberspace in the future? I ask this because there is a book written by two Chinese colonels...

P.V.N. "Unrestricted Warfare."

A.N.A. Exactly, "Unrestricted Warfare," which essentially discusses, among other things, how in the future wars would be invisible, not fought with soldiers, ships, etc. But rather, a significant portion of the conflict would take place invisibly, in cyberspace, attacking those critical infrastructures. Do you see this as the future?

P.V.N. The future will require a lot of imagination and creative work. It's not something that can be fully anticipated at this point. However, warfare itself will undergo drastic changes. In conversations with other high-ranking officers, I often discuss how kinetic conflict still holds precedence over non-kinetic conflict. The non-kinetic conflict we're discussing here is the type that takes place in cyberspace. The logic of conflict has shifted from one combatant engaging another in close combat; that concept is no longer relevant today. Instead, we will see an increasing presence of unmanned devices on the battlefield, such as drones, autonomous systems, and combat robots. These robots may not resemble the relentless terminators we see in movies, but they will possess transport and placement systems for explosives that can be remotely detonated. War will be mediated by machines, and that is the future paradigm. Therefore, if war is mediated by machines, the true nature of warfare becomes one of logic, information, and the flow of information. What we will witness is a situation where a technologically advanced country with disruptive technologies introduces combat robots on a large scale. The ongoing conflict in Ukraine serves as an example of many of these areas we are discussing. However, humans are unable to effectively deal with machines. As a result, the opposing side will deploy their own machines to fight against the initial machines. Humans will be behind these machines. The conflict will be mediated by machines, but overall, in terms of the phenomenon of war, it won't be exclusively machine-based. There will always be a need for soldiers on the ground, among other factors. However, the major confrontations and dynamics of war will occur at this level. This brings the cyber realm's influence into managing this new type of conflict more than ever before. Thus, the importance of cyberspace and cyber defence will grow immensely due to the evolving paradigm of warfare. This aligns with the teachings of Sun Tzu, as those two Chinese colonels I studied and analysed mentioned. Their lessons from Sun Tzu are being applied to the modern era: defeating without fighting and dominating instead of destroying. It's a type of silent war. If we introduce artificial intelligence into this paradigm, we will encounter significant challenges. AI has strong learning capabilities in extreme situations. The delegation of decision-making rights to machines is a trend that will continue to deepen. At that point, humans lose control over what is happening and lack the ability to reverse the course of action effectively. Thus, control must be carefully managed and

calculated to prevent disruptive moments where machines create their own dynamics. We speak of machine learning and the machine's ability to learn. The recent example is GP3, a robot or artificial technology that can generate literary texts and propose solutions when given specific inputs. In fact, there was a competition between a lawyer and an AI to see who could better present arguments to win a case. However, as long as we view humans as machines teaching machines, what happens if we have a machine teaching another machine? How far can this scale? This leads us to the concept of Deepfake, where machines learn from other machines to mimic humans. It's a challenging scenario. This brings us back to the earlier mention of cognitive warfare. We will witness people taking certain actions that are not genuine. There will be wars of narratives, working with ideas and suggestions. If we consider the impact of, for example, the metaverse, where people are immersed in a virtual or augmented reality environment, interacting in a virtual world, the physical loses significance, and what gains significance is the idea or abstraction of the physical. Clearly, we are entering the cognitive realm, which will govern this new type of warfare. At present, real estate is being bought and sold in the metaverse. People are investing in metaverse properties, as if it were a physical space with shopping centres, houses, and more. This is what we're talking about. Have you seen the movie "Surrogates"?

A.N.A. I'm not sure.

P.V.N. Bruce Willis.

A.N.A. Yes, they were... They are all machines, right?

P.V.N. No, they are two individuals who are at home wearing helmets and experiencing a life in a world that is identical to the real world in terms of visuals. They move around as if they were physically moving. They have the same feelings, the same sensory experiences as if they were living in that world, but they are actually lying in bed at home.

A.N.A. Yes, but Bruce Willis is one of those...

P.V.N. He's one of those individuals who wakes up and discovers this paradigm, and it's disturbing, but what we're discussing here...

A.N.A. That's essentially it. It's a...

P.V.N. It's a metaverse. Yes, that's what we're talking about. And it's so immersive that even if someone is told they're not in a physical environment,

they still act and behave as if they are in a physical environment. And that's dangerous because eventually, the sense of where we are interacting gets lost. Whether we are interacting in the real world or the virtual world. In the real world based on the virtual one, right? So, if the virtual is the mediator between the real and another real point, it's not easy to discern. But these are issues that could be doctoral thesis topics, if that's the case.

A.N.A. Well, I imagine so.

A.N.A. The next question is simpler, which is... What kind of damage can a cyber-attack cause today? What is the maximum damage that a cyber-attack can achieve?

P.V.N. A cyber-attack can do things that a kinetic attack could never accomplish. We have a concrete example, which is the destruction of the enriched uranium centrifuges in Iran. No kinetic attack could achieve what that cyber-attack did. On the other hand, it can also carry out subtle attacks, such as introducing an idea into society or influencing a change in voting preferences. We've seen it in the case of Brexit, the U.S. elections, and even the Brazilian elections, where there is controversy surrounding these issues. Therefore, the cyberspace has the ability to physically and socially change the entire world. It has a wide range of effects, ranging from completely disruptive effects at the kinetic level to entirely disruptive effects at the non-kinetic level. It covers a broad spectrum.

A.N.A. I have a question here about human error. Often, the success of a cyber-attack is also due to human error. What is your opinion regarding education and general training, the awareness in the professional environment, in schools, and even programs for the elderly or older people who may not know how to use the internet or computers and can easily fall victim to scams or even a simple incident where an employee of a... of a... Let's say, the SIRESP, finds a USB drive on their desk and doesn't know what it is, but plugs it into the computer, and from that moment on, that USB drive had been left by someone...

P.V.N. They all have instructions not to do that.

A.N.A. It's good that they have those instructions, but how important do you consider the human error aspect in the success of cyber-attacks?

P.V.N. I have a very specific opinion on this, which has to do with the fact that we have an obligation to see everything as a network, with interconnected links. It is the weakest link that will define the security and resilience level of a network. Naturally or invariably, the weakest link is humans. This is due to a lack of training, but also primarily due to a lack of awareness of what is at stake.

It's not just technological awareness; it's a situational awareness of the implications of technology. The social aspect, the functional support of critical infrastructures we mentioned earlier, depends on it. The individual risks I mentioned can easily be carried over to the collective, within a social network, a universe, a work context, a family context, and so on. But my idea is very simple: no one should be allowed to touch a computer without training. And why is that? Because a computer, at this moment, is like a car. Just as we are educated to understand that driving a vehicle requires a driver's license, we need to know what to do, we need to pass an exam for the license. There is a very interesting concept called the ECDL (European Computer Driving License). There used to be ECDL academies, although we don't hear about them as much now, but basically, they provided basic digital skills to every citizen. This should be mandatory before using a tool without knowing the implications of its use. And just as we have to wear a seatbelt, which is not intuitive, but we learn that we have to use it, without using cyber protection or cyber hygiene mechanisms, as it is sometimes referred to, it should not even be possible to turn on the car while driving. It should be a presumption, a baseline that must necessarily exist. And when I talk about a computer, I mean a mobile phone, which is just a summary, but it is a computer in practice. People often lack this perspective. It would require a strong cultural change. But it has to start in schools. When parents give tablets to their children to use, it is important that the children may not take a cybersecurity course, but at least the parents ensure that they respect those basic principles when they hand the devices over, until the children become autonomous in that regard and can take those precautions themselves. It is a cultural, educational, and generational change, but it requires policies implemented at the highest level because society needs to be cyber-resilient. It needs to function at a digital level, but also be cyber-resilient.

A.N.A. I also wanted to ask some questions about your time as the director of the NCI Academy. I wanted to ask if you believe that this academy has had a positive impact nationally in training professionals and individuals who can contribute to cybersecurity and cyber defence in Portugal?

P.V.N. The NATO School, NCI Academy, located in Oeiras, should not be seen as a national property. That is not the objective.

A.N.A. Yes, yes, I know, but in this case, I wanted to know if, in Portugal... because there might be more Portuguese people attending...

P.V.N. But let me explain why. The number of people attending that national school is very small. It's very limited. The school is, in a way, shared with all NATO countries and structures. Portugal is a country among others, among nations. Naturally, it has a great advantage in terms of geographic location. It doesn't incur personal travel costs, etc. Therefore, the ratio of benefiting from and reserving space to train people is more favourable to Portugal because it serves as the host nation for the school. But this effort we're talking about is not only done through the NATO School. It is primarily done through a national

strategy. There is a cybersecurity framework, which the National Cybersecurity Centre has mobilized and was approved as the basis for a project called C Academy, which brings together schools and aims to train people. The ambition is to train 10,000 people in cybersecurity competencies by 2030.

A.N.A. Yes, I noted that in my thesis. It's a program called "e2030," right?

P.V.N. Yes, 2030 is the target defined to provide people with cybersecurity skills.

A.N.A. Yes, yes.

P.V.N. But more needs to be done. Any efforts made are beneficial and always trying to meet the needs. So, significant investment is required.

A.N.A. Have there been any visible effects on NATO since the establishment of the NCI Academy?

P.V.N. Yes, NATO did not have a cyber curriculum. What we did with our project, developed under the Multinational Cyber Defence Education and Training, was to deliver the curriculum we had developed to the NATO School. I had the opportunity and, in a way, played a role in this transition because the school, before being here, was located in Latina, Italy, known as the NATO Communication Information Systems School. It was later transferred and transformed into the NATO Communication Information Academy. We held several meetings for this Multinational Cyber Defence Education and Training project. Within NATO, there were 23 countries participating, along with numerous other organizations, totalling 40 member entities for this project.

A.N.A. 23 countries?

P.V.N. 23 countries. There were countries outside the NATO structure, such as Japan, Macedonia, and Ukraine, which were interested in joining. Within the European Union, all EU member states were involved. At the national level, we had 108 members and 28 organizations, including universities, research centres, and banks.

A.N.A. 128?

P.V.N. 108. It had all the stakeholders: the branches of the Armed Forces, the Cybersecurity and Cyber Defence Centre, several ministries, and universities.

In fact, from that curriculum, a postgraduate program in Cybersecurity and Cyber Defence emerged, which was taught in collaboration with 11 Portuguese universities. The Military Academy served as the scientific coordination and the University of Minho as the pedagogical coordination, but it involved 11 universities and was structured in a completely different way from previous training programs. Usually, what happens is that when there is a training program in classical sciences at a university, the university shapes the training according to its resident expertise, its professors, its research centres, etc. What we did was develop an abstract, unbiased, and structured curriculum based on certain formatting assumptions for the content, etc. Then, we searched for where the national centres of competence were in those areas. The universities were chosen because they were centres of competence in those areas, not because they were all aligned around their own curricula. We completely changed the paradigm. What resisted these efforts the most? The first technical cybersecurity course was launched at IEFP (Portuguese Institute for Employment and Vocational Training) by the ATEC group, part of the Volkswagen Group Training Academy. A series of courses were developed, including a course on strategic decision-making held at the National Defence Institute (IDN) in collaboration with the Military Academy, Crisis Management and Cybersecurity, which includes a final exercise with a team from Estonia that has been connected with us since the first edition. There is a course on cyber operations planning at the Military University Institute, which trains military personnel annually for cyber defence operations and has helped shape a series of courses that are now part of a portfolio of a project born at the Military Academy here, called the Cyberacademia Innovation Hub. This project was even proposed as the headquarters of the DIANA network, which NATO established to fund start-ups and innovative components. It is relevant.

[END]

Appendix I.b – Original Portuguese

[START]

Paulo Viegas Nunes: Falar só da cibersegurança no contexto da NATO numa lógica de alianças de Portugal é redutor. É redutor porque, por outro lado, a União Europeia está a iniciar um esforço semelhante e porque existe um outro elemento integrador daquilo que é a visão estratégica da União Europeia e da NATO e que normalmente é consolidada nas Cimeiras através de uma declaração de conjunto que ocorreu também na última Cimeira e que foca os aspetos de cooperação. Porquê que eu refiro isto? Porque Portugal, sendo um país que é membro das duas organizações internacionais, não pode só focar a sua orientação estratégica e política para a área da cibersegurança e da ciberdefesa por um dos lados. Tem que ir equidistante dos dois e tem toda a vantagem que aquilo que faça esteja perfeitamente alinhado com os objetivos definidos. Aliás, não é um caso único. Temos 20 e poucos países na mesma situação. Até há pouco temos o que eram 23, agora são 22, porque o Reino Unido saiu no caso da União Europeia. Mas isto para dar conta que uma dissertação de mestrado viveria melhor com esta latitude. Porque é o quadro das alianças. É a visão externa da política externa, nacional. Portanto, na prática, o que estamos a falar é de cibersegurança numa lógica de visão estratégica nacional e depois internacional, no quadro de segurança e defesa. O que liga com o tema mais tarde. Portanto, a segurança e defesa de Portugal é arquitetada em termos de visão em torno destes dois pilares no âmbito da segurança e defesa. Eu tenho feito.

António Neves Almeida: Tenho algumas referências na minha tese sobre a União Europeia, mas tenho de focar mais na parte da NATO e nas estratégias nacionais de alguns países sobre como é que têm adaptado, ou seja, como é que têm feito a sua ciberestratégia? Porque há uns países que têm mais, por exemplo, Reino Unido, Estados Unidos, que têm uma estratégia mais ofensiva na sua cibersegurança. Enquanto outros países têm como... Defensiva. Exato. Como Alemanha, Espanha, etc. E por vezes por razões legislativas e políticas, como está dividido os poderes nesses países. E às vezes também por meio, simplesmente porque o próprio país não tem meios para ter uma segurança mais ativa.

P.V.N. Não tem a ver com a natureza da ciberdefesa, tem a ver com a vocação, a visão do papel da ciberdefesa. A capacidade ofensiva é fundamental para uma boa defesa. Sem essa capacidade de dissuasora e garantir a defesa, não há defesa possível.

A.N.A. As primeiras perguntas são muito simples, muito básicas, que é como é que vê o estado da arte da cibersegurança e da ciberdefesa de uma forma geral? Como é que vê em termos nacionais? E como é que vê em termos da NATO?

P.V.N. A nível de maturidade da visão estratégica da NATO é superior à nossa. Essencialmente por uma razão. O nosso edifício está um bocadinho atrasado em termos de construção. Como julgo que sabe, a estratégia nacional de ciberdefesa só foi aprovada em 2 de novembro, portanto é muito recente quando a visão estratégica e a lógica subjacente ao levantamento de capacidades noutros países já tem muito tempo. Em alguns casos até década, é mais do que uma década em alguns casos. Há países como os Estados Unidos, que montaram o seu ciber-comando em 2009, em 2011 já o tinha mobilizada. Comparativamente com o estado em que nós estamos neste momento, já vamos em 2023, foi aprovado em 2022, novembro, final do ano, é difícil, nós consideramos que a maturidade é a mesma, não é? Uma disseminação muito forte. E os Estados Unidos são um parceiro muito preponderante no âmbito da NATO. Significa que a lógica estratégica e operacional da NATO vem muito alinhada com aquilo que é a visão da política de segurança e defesa dos Estados Unidos. Sendo que a política de segurança e defesa tem um valor de defesa muito forte, é um ator global, projeta poder à escala global e, como tal, tem, sob o ponto de vista também do exercício desse poder a necessidade de ter capacidades robustas em determinadas áreas e o ciberespaço é hoje em dia é uma área prioritária da projeção de poder potenciado muito pelo domínio transversal que o ciberespaço constitui e pela natureza dos efeitos que se produzem nesta tipologia de domínios porque na prática o que estamos a falar é efetivamente de um instrumento de guerra de natureza híbrida em que a lógica multi-agência decorrente da transversalidade que o ciberespaço tem é ela própria um grande desafio. E talvez o maior desafio para a humanidade. Portanto, dentro da maturidade, maturidade nacional, julgo eu, está um bocadinho aquém. Por outro lado, a parte orgânica, o Estado Maior General das Forças Armadas, no âmbito da sua última... do seu decreto parlamentar decorrente da lei orgânica no caso das forças armadas, a LOBOFRA, que foi revista e aprovada, contempla um comando para as operações nos diversos passos, para a ciberdefesa. A organização não seria, na minha opinião, a melhor ainda, porque está subdimensionada, por um lado, e depois, sob o ponto de vista da relação de comando, não está no sítio certo. Se levarmos à prática a doutrina vigente, tanto ao nível americano como ao nível da NATO, todo o domínio de operações tem, de um ponto de vista de comando e controle, um comando e controle estruturado em torno desse domínio. Significa que, na prática, o que eu estou a dizer é que o comando do ciberespaço devia ser semelhante ao comando das forças terrestres, da força aérea, ou comando da marinha ou comando naval. Portanto, devia haver um comando do ciberespaço na mesma linha. E esse comando do ciberespaço devia se ligar diretamente ao comando de operações conjuntas para fazer a articulação do leque de utilização necessário para os vários domínios operacionais numa lógica até de multi-domínio de implementação da projeção da força militar. Outra área que eu julgo que em termos nacionais precisa de crescer é o uso das componentes militares. Nós neste momento temos uma estrutura no âmbito da cibersegurança que está mais ou menos consolidada, que tem o Centro Nacional de Cibersegurança no centro e depois tem uma arquitetura ad hoc que está constituída, que se chama G4, que em caso de uma

operação disruptiva de grande dimensão, reúne. E o G4 é composto por quem? É composto pela estrutura de cibersegurança, personalizada no Centro Nacional de Cibersegurança, que é composta pela parte da investigação policial ou criminal com a Polícia Judiciária e com o momento C3T, que é a Unidade de Combate ao Crime Tecnológico da Polícia Judiciária, pelo CIS, Sistema de Informações e Segurança, e pelas Forças Armadas, do Centro de Ciberdefesa, que ainda não há estabelecido o Comando de Ciberdefesa, que ainda está a implementar. O que é que isto traz? Isto traz uma articulação ao nível da cibersegurança. Se houver uma intervenção da ciberdefesa, ou seja, se o tipo de efeito for destrutivo ou disruptivo em larga escala, a coordenação deste tipo de resposta nacional passa para o domínio da defesa, já não ao domínio da segurança. E aí não há estrutura para atuar. Podemos dizer que o G4 serve para a cibersegurança, serve para a ciberdefesa. É verdade, mas sob o ponto de vista político, a tutela é completamente diferente. O caso concreto, o Centro Nacional de Cibersegurança depende diretamente da presença do Conselho de Ministros. O caso da ciberdefesa depende do Ministério da Defesa, através, naturalmente, do Estado Maior General das Forças Armadas. No Estado Maior General das Força Amadas não existe coordenação interministerial, sendo o que os ingleses designam por "all of state", uma resposta agregada, multi-agência, multidimensional, e multissetorial, isto carece de uma tomada de decisão nacional ao mais alto nível, que é a presidência do Conselho de Ministros. E a única entidade que tem acesso à Presidência do Conselho de Ministros é o Centro Nacional de Cibersegurança. Significa que a resposta nacional está predominantemente canalizada para o domínio da cibersecurança. Se houvesse a necessidade de ativar a capacidade de ciberdefesa, o que nós tínhamos de ter é um plano de operações previamente aprovado, articulado entre todos os ministérios.

A.N.A. E não temos isso.

P.V.N. Não temos. Nem temos capacidade com a estrutura conforme está de garantir que isso é feito de uma forma célere. E é essa parte que fragiliza a articulação da ciberdefesa dentro de um quadro que obriga a uma atuação transversal. Portanto, a minha lógica consubstancia-se no facto, e eu tenho descrito isso, publiquei uma visão nesse sentido, nós precisarmos de um Conselho Nacional de Defesa do Ciberespaço. Nós neste momento temos um Conselho Nacional de Segurança do Ciberespaço, onde estão as várias entidades envolvidas para uma crise no âmbito da cibersegurança mas se tivermos uma crise no âmbito da ciberdefesa, nós precisamos de reunir as várias entidades sobre a presidência ou sobre a coordenação do Ministério da Defesa. Não pode ser a mesma linha que temos para o caso da cibersegurança. Portanto, é esta coordenação que falta na construção do edifício.

A.N.A. E acha que ainda estamos longe de chegarmos a esse ponto?

P.V.N. Não muito longe. Estamos a cumprir o caminho, não é? Neste momento, e eu julgo que devemos estar de alguma forma satisfeitos com este trajeto, aquilo que estamos a fazer é construir o edifício. Construímos ou identificámos a estratégia de ciberdefesa, não tínhamos, já temos. Há um plano de implementação da estratégia de ciberdefesa, agora é a série. Antes só havia

linhas orientadoras para a estratégia de ciberdefesa, agora não. Agora é um plano a sério, é o ENCFAC, que é o Estado Maior Geral das Forças Armadas, que têm a responsabilidade da sua implementação. E falta agora a criação deste órgão, que é um nível político. É um órgão de nível político, não é um órgão de nível militar. Tem de ser um nível de defesa. Não pode ser um nível das Forças Armadas. É curioso porque o modelo que eu desenvolvi é um modelo pirâmide. E o modelo pirâmide ajuda a explicar isto. O que é que temos no modelo de pirâmide? Temos duas pirâmides, uma da cibersegurança e outra da ciberdefesa, em termos nacionais, que depois por nível se vão ligando. E aí fica claro o que estou a dizer em termos de ligação e coordenação, porque a coordenação técnica, a coordenação operacional, a coordenação estratégica e a coordenação política tem que existir. Se virmos isto como uma pirâmide por leias, por camadas, isto fica mais claro. E depois temos que efetivamente construir a lei política da ciberdefesa, que não existe ainda. E essa é a lei que falta. O que é que isto leva? Leva a que sempre que o Estado tem de discutir assuntos, seja no âmbito da NATO, seja no âmbito da União Europeia, que toquem a área da ciberdefesa, ao nível político, quem é que vai é a área da cibersegurança. Ou seja, nós temos de ter interlocutores dentro da componente internacional no sítio certo. O modelo das pirâmides é completado com duas outras pirâmides que circundam estas pirâmides nacionais e que mobilizam muito a visão do Estado para as duas dimensões. No âmbito político e no âmbito da cibersegurança, o nosso parceiro primordial e central é a União Europeia. Portanto, há uma pirâmide da União Europeia para a cibersegurança. No caso militar, a nossa pirâmide é a pirâmide NATO. E aí há outra pirâmide. Portanto, isso significa que se ao nível NATO, quando falarmos da área da ciberdefesa, nomeadamente ao Comité de Ciberdefesa, que é o CDC da NATO, tivermos de tomar posições oficiais, não pode ser a cibersegurança a ir de alguma forma representar o país nesse domínio. Tem de ser alguém, do nível político, efetivamente, mas na área da ciberdefesa. Falta esta parte. O modelo da pirâmide só vem isto muito claro. Encontrei esse modelo explicado e mapeado no livro que eu escrevi quando fiz o curso de promoção oficial general ultimamente está a necessidade do levantamento de uma estratégia militar de ciberdefesa. É uma coisa diferente da estratégia nacional de ciberdefesa.

A.N.A. Como é que se chama esse livro?

P.V.N. Está no IUM, no Instituto Universitário Militar e foi o meu trabalho de investigação de final do curso de promoção oficial general e a coleção Ares 28, acho eu.

A.N.A. Isso acabou por também responder às duas próximas perguntas. Uma das próximas perguntas que era o que é que faltava em termos de segurança e defesa em termos nacionais? E depois também a outra era o que é que faltava ainda, na sua opinião, no âmbito da NATO? Porquê que acha que falta a NATO fazer? A NATO está capaz de se defender contra outras potências, se ainda falta muito para andar...

P.V.N. A NATO tem uma ambiguidade construtiva. O que é que é a ambiguidade construtiva? É a utilização do Artigo 5º em caso de ciberataque. O problema maior dos ciberataques é que os ciberataques são permanentes. Não

há paz, guerra. São um nível de intensidade que pode escalar imediatamente de um momento para o outro e que se não tiver um mecanismo de reserva ou de controlo do seu ponto de vista daquilo que é a evolução de uma crise, obriga a declarar o Artigo 5º, basicamente. E a NATO não pode fazer isso, senão está constantemente a declarar a guerra. É algo que não é aceitável, sob o ponto de vista da estratégia. Porque a NATO tem uma estratégia defensiva, tem assumidamente uma estratégia defensiva. Tem estado a mudar com o conflito da Ucrânia. Portanto, isto tem vindo a sofrer aqui certos ajustes. Mas significa que não renega a utilização de meios ofensivos. Então tem uma estratégia que passa por um conceito de Strategic Production of Effects. Basicamente o conceito é a produção de efeitos de países em prol da NATO. Os países cedem à NATO as suas capacidades ofensivas e a NATO se tiver que atuar ofensivamente com capacidades ciber, não atua como NATO, pede a um país que tem capacidades para atuar como a "NATO da NATO". Então é uma coisa assim um bocadinho diferente da nossa visão tradicional de utilizar o poder militar, mas é efetivamente isso que acontece. Portanto, o que é que falta ainda construir no âmbito da NATO? Para já esta noção clara do que é o domínio operacional ciberespaços com o comando estratégico para o ciberespaço. A NATO tem comandos estratégicos, está dividida por comandos estratégicos e esses comandos estratégicos normalmente especializam os meios aéreos e os meios específicos terrestres, etc. Falta o comando estratégico para a Iniciativa de Ciência. O específico para a área da ciberdefesa. Neste momento, a parte da ciberdefesa, existe o CIOC, que é o Cibercomando Operacional dentro do comando ou do departamento de CIS. É a mesma pessoa que faz a dupla ligação, mas não é um comando. É um plano operacional de per si. Isso fará o seu caminho, naturalmente, porque começa a crescer muito a capacidade disruptiva e destrutiva desta área, deste domínio, e vai crescer mais e mais um planeamento integrado. Mas tem de ser robustecido, ao nível não individual de cada país, que é o que está a acontecer, mas também ao nível da defesa coletiva, no caso específico da NATO.

A.N.A. Pode-se dizer até que isso, de alguma forma, já está a acontecer, através do centro de formações na Estónia, através da academia do NCI.

P.V.N. Não é a mesma coisa. Aquilo que estamos a falar é um comando operacional. O que me está a falar é de um centro de excelência, de dar treinos, doutrina, etc. No caso especial aqui da academia de Oeiras, NCI Academy, o que estamos a falar é uma escola que dá formação também nessa área. Não é uma escola "ciber" pura. Eu não sei se tem essa informação, mas eu fui o primeiro comandante dessa escola aqui e acompanhei na altura esse processo de lançamento de um currículo ciber na escola. Aliás, isso veio de um projeto que Portugal liderou e que eu também fui gestor desse projeto. Era um projeto que se chamava Multinational Cyber Defense Education and Training. Era um projeto Smart Defence da NATO, que, por coincidência, desenvolveu um currículo que foi comum também à União Europeia. Porque Portugal também foi líder da Cyber Defence Discipline, no caso específico da União Europeia, do EUMTG, que é o EU Military Training Group. E Portugal liderava as duas partes. Liderávamos o Multinational Cyber Defense Education and Training, o Cyber Defence Discipline da União Europeia e construímos cá em Portugal uma extensão deste grupo. Conseguimos a um determinado momento que, tendo um

plano de trabalho alinhado, o currículo também alinhado, tudo o que fossem iniciativas produzidas em cada um destes três domínios, projetava automaticamente para os outros. Criámos um sistema de cooperação muito interessante e organizámos aqui em Lisboa, nas instalações da Academia Militar na Amadora, vários seminários dos projetos de Smart Defence na área de Ciber, no caso específico da NATO, com colaboração com a União Europeia e com os outros parceiros. Mas não é a mesma abordagem termos um centro de excelência, termos uma escola e termos um núcleo operacional. São coisas diferentes.

A.N.A. Não, o que eu quis dizer com isso era como... Embora não haja algo central, já está de certa forma... Ou seja, não há... Temos um país a treinar-se a si mesmo, a desenvolver as suas próprias capacidades. E, desta forma, poderíamos eventualmente dizer que a NATO está a ajudar os países a treinarem-se uns aos outros, a ajudar a treinar uns aos outros, através desses centros de excelência.

P.V.N. O conceito é defesa coletiva. Para haver defesa coletiva, para haver colaboração, tem de haver doutrina e treino comum, senão as pessoas não conseguem atuar em conjunto. É isso que estamos a falar.

A.N.A. Tinha aqui outra pergunta. Essencialmente era se a situação que nós temos agora, de cada país se desenvolver a si mesmo, se prejudicar a NATO, se prejudica a capacidade da NATO de se defender ou se no futuro seria melhor a NATO ter, no fundo também já acabou por responder, mas se devia ter uma estrutura central, uma política, uma estratégia unida para todos os países?

P.V.N. Tem de ser. Aliás, a área do ciberespaço é um domínio de soberania, não podemos esquecer disso. Cada país tem de ser soberano e para ser soberano tem de ser autónomo, na componente de defesa desse domínio. Aliás, é uma responsabilidade inalienável. Não é daquelas responsabilidades que se possam delegar a terceiros. É fundamental que cada país sinta isso. Mas da mesma maneira como percebem a dimensão da defesa coletiva, que é uma defesa cooperativa, não é uma defesa isolada ou de um país. É um desporto de equipa, como dizem os ingleses. Naturalmente tudo isso carece de atuação conjunta. E é por isso que a NATO tem plano de exercícios, tem doutrina. A doutrina é princípios de atuação que são partilhados por todos. Portanto, se nós tivermos a noção de que temos de trabalhar todos da mesma forma, treinarmos a forma como trabalhamos, vamos juntar sinergias. A diferença disto é que cada um faz a sua, cada um desenvolve os seus exercícios e não há garantia nenhuma que as coisas depois vão convergir. Mas a NATO tem de fazer isso. Se quiser atuar com unidade de esforço e unidade de comando, que é o princípio fundamental.

A.N.A. Considera que Portugal ainda está em risco de ser um país mero executante das estratégias ditadas de nações ou organizações líderes nesta área?

P.V.N. Eu acho que considero que Portugal tem o dever e tem justas expectativas de ter a sua autonomia e a sua afirmação própria neste domínio. Aliás, eu em conversa com um amigo do Reino Unido que estava ligado ao desenvolvimento da capacidade nacional de ciberdefesa, eu perguntei-lhe

"então como é que vocês conseguiram fazer o Mindset ou o 'mindshift' neste caso para melhorarem este tipo de capacidades e criar equipamentos para o desenvolvimento?" Ele deu uma resposta que eu, depois de pensar, considerei que de facto fazia todo o sentido. Eles explicaram a necessidade de uma capacidade destas com base numa análise macroeconómica. Ou seja, a economia do Reino Unido em 2030 está a 70% digital. Ou seja, se o ambiente ou o ecossistema digital for atacado e, como tal, não estiver disponível, o país colapsa, do ponto de vista económico. Cresce a isto as preocupações das infraestruturas críticas e do conceito de resiliência que teve um grande penduro durante o processo pandémico. A pandemia de Covid-19 trouxe aos vários Estados e às várias organizações internacionais grandes desafios em termos de sobrevivência na área digital e de transformação. Não foi só sobrevivência, foi transformação. Portanto, deixou de se falar tanto em segurança e falou cada vez mais, passa a se falar, segurança e resiliência. Resiliência é uma palavra muito chave neste contexto. E é por essa razão que a componente ciber é fundamental, é condição necessária e às vezes não o suficiente, mas é condição necessária para haver resiliência digital de um Estado. Portugal está claramente com um nível de ambição extremamente forte naquilo que é a sua visão, transformação e transição digital e tem que, para de alguma forma arquitetar uma estratégia de afirmação neste domínio, tem de contemplar uma segurança e defesa muito forte, porque senão depois torna-se vulnerável, torna-se frágil. É o caso dos nossos cartões, nós deixamos de andar com dinheiro físico praticamente dentro da carteira, o cartão acaba por ser a carteira virtual, mas se não há forma de fazer um pagamento parou economia. Estagnou. Não há trocas comerciais, os poucos que têm ainda dinheiro físico dilui-se o dinheiro físico nos primeiros segundos os primeiros minutos da interrupção dos fluxos económicos digitais e perdeu tudo. Depois temos o sistema escada de controle da eletricidade dos gases, das águas os sistemas de controle de tráfego, que é aéreo, só para falar de uns quantos as próprias comunicações podem ser alvo de ciberataques e o nosso país tem sido alvo de vários ciberataques nos últimos meses. O ano passado foi muito fértil, mas este ano já começámos com, de alguma forma, uma afirmação, uma tendência que cresce, não vai reduzir-se. Tudo isto precisa de proteção, precisa de defesa, para ser resiliente. Portanto, Portugal não pode, de maneira nenhuma, descurar esta componente e tem de ter um plano muito consistente para lá chegar. Os recursos humanos são muito limitados e naturalmente carecem de um período de formação muito dilatado.

A.N.A. Também aproveito agora que faço também outra pergunta que era também especificamente para si, que era que tinha, em 2014 escreveu um artigo na revista militar com o Tenente-Coronel Piteira Natário, onde fala das infraestruturas críticas, e eu queria perguntar se, nove anos depois, considera que essas tais estruturas críticas estão mais salvaguardadas hoje do que estavam antigamente? E se sim, se ainda é o suficiente ou se ainda há mais para fazer, naturalmente há sempre mais para fazer, mas se considera que ainda há muito mais para fazer?

P.V.N. Eu, em junho do ano passado, escrevi outro artigo para a EuroDefence que foi publicado na edição nacional e depois na edição internacional com o engenheiro Paulo Moniz, do grupo EDP. E aquilo que eu julgo que passou a existir foi um melhor entendimento daquilo que são as fragilidades e as

interligações das várias infraestruturas críticas. Porque há de facto situações muito diferentes entre umas e as outras. Isso é incrível. E a União Europeia chamou assim esse plano. Está a lançar legislação específica para garantir os níveis mínimos de resiliência, não só infraestruturas críticas, mas aquilo que ela designa, a União Europeia, por serviços essenciais. Podem não ser só infraestruturas, podem ser serviços essenciais, tudo. Pode ser a segurança social, por exemplo. Pode ser o sistema informático. Pode ser o fisco, pode ser a base de dados do património, pode ser a base do Ministério da Justiça, a base de dados do Ministério da Justiça, tudo isto pode, de facto, ter um valor patrimonial não tangível, não é? Não é físico, infraestrutural, mas é de facto, um serviço essencial para manter a sociedade a funcionar. Além disto, do lado da NATO também houve um esforço muito consistente neste domínio. A NATO chama-lhe os pilares base da resiliência. Houve uma declaração conjunta, NATO e União Europeia, na Cimeira de Varsovia, em 2016. E define uma série de setores em que se torna necessário garantir a colaboração entre a componente militar e aquilo que é designado nesses documentos por "civil preparedness", preparação da sociedade civil com o apoio das forças armadas para garantir a resiliência dos Estados. E levou isto para o patamar NATO. Ou seja, não é só a resiliência dos Estados, é a resiliência da própria estrutura da NATO. E por isso que eu estou a mencionar este caso? Porque este caso tem um paralelismo com o caso da União Europeia. A União Europeia também deu estes passos, quer dizer, é uma imposição, é uma recomendação aos Estados membros, mas também ela própria quer atingir uma resiliência comum. Portanto, por exemplo, o mercado comum de energia elétrica, o mercado comum do gás, energético, fala-se de uma concertação e atuação conjunta das várias entidades que trabalham com proteção civil, por exemplo, no caso da União Europeia. Portanto, há uma consciência que a emergência e a proteção é devida e é necessária para lá de fronteiras, não é só dentro das fronteiras e que se calhar, dada a interconexão das redes, de todos os tipos de redes, desde a energia até a comunicações, etc. A proteção não pode ser uma proteção perimétrica interna, tem de ser uma proteção agregada e de ecossistema. Isso muda a mentalidade das pessoas. E nesse nível de maturidade eu julgo que evoluímos de alguma forma.

A.N.A. Considera que o ciberespaço e a dependência do ciberespaço é hoje bastante importante para o dia a dia da NATO e quando digo dia a dia da NATO, também refiro-me a operações militares da NATO, onde hoje cada vez mais dependem do ciber para efetuar essas operações. Se considera que a dependência tem crescido? Se hoje em dia é algo ainda mais importante que deve ser protegida da forma mais indicada?

P.V.N. Sim, eu julgo que é transversal, não é só a NATO, são todas as instituições, em todos os países, a tendência cresce quanto maior é a ligação a redes, porque este tipo de ameaças trabalha em rede e é a rede que de alguma forma maximiza e promove a difusão deste tipo de ameaças. Para lá da parte de crescimento ao mesmo nível, ou seja, infraestrutural, nós temos outro tipo de crescimento, que esse sim está a ser visível e está a evoluir de uma escala sem precedentes, que tem a ver com o crescimento ao nível da pirâmide cognitiva. Ou seja, nós estamos a passar de um ataque puramente infraestrutural, por um ataque quase nível físico, quando eu falo físico não estou a falar de

infraestrutura de jogo, estou a falar de bits e bytes, estou a falar de fluxos de informação, para um ataque que tem a ver com aquilo que é a estrutura da informação, com a sintaxe, a forma como os caracteres e a informação se encontram estruturada, isto ao nível da guerra de informação e da desinformação, por consequente. Mas depois, a outra componente que vem em montante desta, que é a parte da cognição. Que é nós entrarmos numa lógica de rede em que aquilo que nós vamos promover e vamos influenciar não é tanto já a parte sintática, ou seja, os caracteres e a forma como a informação vem, mas sim a parte semântica, que tem a ver com o significado da informação e a forma como nós vamos interagir a esse patamar. Isto na prática significa transformar uma busca de ocorrência de caracteres na busca de ideias. E significa que nós, quando promovemos a difusão e manipulamos um determinado ambiente, que tem o suporte do ciberespaço, o que nós vamos fazer é manipular crenças, manipular perceções em vez de manipular estruturas de informação. E isto faz, efetivamente toda a diferença.

A.N.A. Como é que considera a importância do ciberespaço no futuro? Eu pergunto isso porque há um livro escrito por dois coronéis chineses...

P.V.N. "Unrestricted Warfare"

A.N.A. Exato, "Unrestricted Warfare", que essencialmente fala, entre outras coisas, de como no futuro as guerras seriam invisíveis, não seriam de soldados, navios, etc. Mas que uma grande parte do conflito seria feita de forma invisível, no ciberespaço, atacando as tais infraestruturas críticas, se vê isso como sendo o futuro?

P.V.N. O futuro vai ter muito de imaginação e criação por fazer ainda. Não é algo que já esteja completo hoje em termos de possibilidade que temos de o antecipar. Mas a guerra em si vai mudar drasticamente. Eu muitas vezes em conversas com outros oficiais generais, porque normalmente eu falo de oficiais generais, porque os oficiais generais têm escolas do ponto de vista do conflito. Muitas vezes fala que o conflito cinético ainda tem prevalência sobre o conflito não cinético e o conflito não cinético é este tipo de conflito que estamos aqui a falar e eu dou como exemplo, ok? A lógica do conflito deixou de ser um combatente aproximar-se de outro combatente por lutar corpo a corpo, isso perdeu sentido hoje. Aquilo que nós vamos ter mais e mais são dispositivos não tripulados no campo de batalha vamos ter drones, vamos ter sistemas autónomos, vamos ter robôs de combate que podem não ter a função tipo um exterminador implacável que vemos aí nos filmes, mas têm sistemas de transporte, sistemas de colocação de explosivos em determinados locais que são detonados remotamente. A guerra vai ser intermediada por máquinas. Esse é o paradigma do futuro. Portanto, se a guerra vai ser intermediada por máquinas, a verdadeira guerra é uma guerra de lógica, uma guerra de informação e de fluxo de informação. E se nós olharmos, aquilo que nós vamos ter é, em determinado momento, um país que esteja tecnologicamente mais evoluído, com tecnologias disruptivas, a dar um passo em frente para introduzir robôs de combate em larga escala. Aliás, o conflito da Ucrânia tem sido palco de muitas destas áreas que estamos aqui falar. Mas o que vai acontecer é que o ser humano não consegue depois lidar com a máquina. E o que é que vai acontecer é que o outro lado vai

colocar outra máquina a lutar com a máquina. E atrás das máquinas estão os seres humanos. O conflito vai ser intermediado por máquinas, mas a guerra como um todo em termos de fenómeno vai ser muito, não vai ser exclusivamente, vai sempre ser necessário o soldado no terreno, etc. Mas os grandes confrontos, as grandes dinâmicas, os grandes conflitos vão se travar a este patamar. Isto traz muito mais impacto da área cyber na gestão deste novo tipo de conflitualidade do que existia antes. Portanto, a importância do ciberespaço e da ciberdefesa vai crescer desmesuradamente por via daquilo que vai ser o paradigma da guerra. A evolução do paradigma da guerra. E isto vai ter muito, como dizem os esses dois coronéis chineses, que eu estudei e analisei, de rebuscar os ensinamentos de Sun Tzu para a era moderna. Derrotar sem combater. Dominar em vez de destruir. É uma guerra em quase que silenciosa. Se nós introduzimos a inteligência artificial neste paradigma, vamos ter grandes problemas. Porque a inteligência artificial tem uma aprendizagem muito forte em situações extremas. A delegação dos direitos de decisão em máquinas é algo que vai ter tendência a aprofundar. E aí o ser humano perde o controle sobre aquilo que está a acontecer e não tem capacidade depois de um determinado momento de reverter aquilo que está efetivamente a fazer. Portanto o controle vai ser um controle que tem que ser musculado e muito bem calculado para que não haja aqui momentos desruptivos em que as máquinas criem dinâmica própria. Nós falamos do Machine Learning e da capacidade da máquina a aprender, fala se agora do GP3, que é o tal robô ou a tecnologia artificial que nós damos um determinado tipo de frase e input e ela produz textos literários e de alguma forma produz soluções. Aliás, a última competição entre um advogado e a inteligência artificial, para ver quem é que esgrimia melhor os argumentos para ganhar a causa. Mas isto enquanto nós pensarmos o ser humano como uma máquina. O ser humano a ensinar a máquina. Então e se nós pusermos uma máquina a ensinar a uma máquina? Quanto é que isto escala? Aliás, há uma coisa que se chama Deepfake. Deepfake é uma máquina aprender com uma máquina. A mimetizar os seres humanos, isto vai ser muito desafiador. E aqui entramos naquilo que eu mencionei há pouco. Estamos a entrar na guerra cognitiva. Nós vamos ver uma pessoa que está a desenvolver uma determinada ação e não está a fazer verdadeiramente. Nós vamos ter guerras de narrativas. Vamos trabalhar com ideias, com sugestões. E se importarmos as pessoas e procurarmos analisar o impacto que tem, por exemplo, o metaverse em que as pessoas vão estar ariadas na envolvente física, vão ter um capacete de realidade imersivo ou virtual e que vão interagir num mundo virtual o físico perde significado e o que ganha significado é a ideia ou a abstração do físico. Portanto entramos claramente na parte cognitiva, vai ser a parte cognitiva que vai gerir. Neste momento estão se a comprar terrenos no metaverse. Não sei se tem consciência disso. Está a se vender imobiliário no metaverse. Como se fosse um espaço físico. Centros comerciais, casas... Estamos a falar disto. Já viu um filme que se chama "Os Substitutos" ou "Os Substitutos"?

A.N.A. Não sei.

P.V.N. Bruce Willis.

A.N.A. Sim, eram... São todas máquinas, não é?

P.V.N. Não, são duas pessoas que estão em casa com dois capacetes e que estão a viver uma vida num mundo que é igual ao mundo real, a imagem e que se deslocam como se estivessem fisicamente a deslocarem-se. Têm os mesmos sentimentos, a mesma sensorização como se estivessem a viver esse mundo, mas estão em casa deitados numa cama.

A.N.A. Sim, mas o Bruce Willis é um desses...

P.V.N. Um destes indivíduos que acorda e descobre este paradigma, e é perturbador, mas o que estamos a falar...

A.N.A. É essencialmente isso. É um...

P.V.N. É um metaverse. É, mas é isso que estamos a falar. E depois é tão condicionador que a pessoa, por muito que lhe digam que não está num ambiente físico, a pessoa age e atua como se estivesse num ambiente físico. E isso é perigoso. Porque depois às tantas, perde-se a noção de onde é que estamos a interagir. Se estamos a interagir no real, no virtual. No real com base no virtual, não é? Portanto, se o virtual é o triangulador entre o real, entre um ponto real e o outro, não é? Não é fácil. Mas são questões que são teses de doutoramento se for acaso isso.

A.N.A. Pois, imagino que sim.

A.N.A. A próxima também é mais simples, que é o... Que danos é que um cyber ataque hoje consegue fazer? Qual é o máximo que um cyber ataque consegue alcançar em termos de danos?

P.V.N. O cyber ataque pode fazer algo com um ataque cinético nunca faria. Temos um exemplo concreto que é a destruição dos centrifugadores de urânio enriquecido no Irão. Não houve ataque cinético nenhum que conseguisse fazer o que aquele ataque fez. E por outro lado consegue fazer ataques tão subtis como introduzir uma ideia numa sociedade. Provocar a mudança do sentido de voto. Temos o Brexit, temos as eleições norte americanas, temos as eleições até brasileiras, que se fala tudo isto em termos de controvérsia. Portanto, o ciberespaço tem capacidade para mudar fisicamente e, sob o ponto de vista conjuntural, socialmente, todo o mundo. É, efetivamente, uma gama de efeitos muito alargada. Desde efeitos absolutamente disruptivos de nível cinético até efeitos completamente disruptivos do ponto de vista não cinético. Tem um espectro alargado.

A.N.A. Tenho esta pergunta aqui sobre erro humano. Muitas vezes o sucesso do ciber ataque é também devido ao tal human error. Qual é a sua opinião relativamente à educação e formação geral, ao tal awareness no meio profissional, nas escolas, até programas para os mais idosos, mais velhos, que não saibam mexer na internet ou não saibam mexer nos computadores e podem facilmente cair em esquemas, podem cair em... Até um simples facto de um funcionário de uma... De um... Agora, por exemplo, aqui do SIRESP encontra uma pen em cima da sua secretária e não sabe o que é, e enfia no computador e a partir desse momento essa pen tinha sido deixada por alguém...

P.V.N. Têm todos instruções para não fazer isso.

A.N.A. Ainda bem que têm essas instruções, mas, que importância dá a essa parte do human error no sucesso de ciber ataques?

P.V.N. Eu tenho uma opinião muito própria sobre isso, que tem a ver com o facto de nós termos a obrigação de ver tudo como uma rede e como uma rede que é com elos. É o "elo" mais fraco que vai definir a segurança e o nível de resiliência de uma rede. O "elo" mais fraco, naturalmente ou invariavelmente, são os seres humanos. Por défice de formação, naturalmente, mas também e essencialmente, sobretudo, por desconhecimento daquilo que está em causa. E é uma awareness, não é uma awareness tecnológica apenas, é uma awareness situacional das implicações da tecnologia. A parte social, a parte funcional do suporte das infraestruturas críticas que falámos ainda há pouco. Depende disso. E aquilo que eu introduzi como risco, individualmente, pode ser transportado facilmente para o coletivo, numa rede social, num universo ou num contexto de trabalho, num contexto familiar, para aí adiante. Mas a minha ideia é muito simples: ninguém devia ser autorizado a tocar num computador sem ter formação. E porquê? Porque o computador, neste momento, é como se fosse um carro, como uma viatura nós somos educados, naturalmente, a perceber que a condução de um veículo carece de uma carta de condução. Temos de saber o que fazer, temos que ter um exame de carta. Há um conceito muito interessante que é o conceito ECDL, que é o "European Computer Driving License". Havia uma série de academias ECDL, agora já não se ouve falar tanto, mas basicamente eram as competências básicas digitais que eram fornecidas a cada cidadão. Isto devia ser obrigatório, antes de passar a usar um meio sem saber as implicações da utilização do meio. E assim como nós temos de usar cinto de segurança, não é intuitivo, mas aprendemos que temos de usar. Sem usar mecanismos de proteção ou de higiene cibernética, como de vez em quando também é dito, não devia ser possível ligar sequer o carro ao conduzir. Tinha de ser um pressuposto, uma baseline, devia necessariamente existir. E quando eu falo de computador, falo de um telemóvel, que é um sumário só, mas que é um computador na prática. É essa visão que as pessoas muitas vezes não têm. E isso passava por uma mudança cultural forte. Mas tem de começar logo nos bancos da escola. No momento em que os pais dão os tablets às crianças para usar, convém que elas não tirem um curso sobre cibersegurança, mas pelo menos que os pais garantam quando lhes passam para a mão, aqueles princípios base são respeitados, até elas terem autónomas nisso e poderem tomar essa precaução por elas próprias, mas é assim, é cultural, é educacional, é geracional, também, mas obriga a medidas com políticas, eu diria, consertadas ao mais alto nível, porque a sociedade é ciber-resiliente. É funcional num nível digital, mas também ciber-resiliente.

A.N.A. Queria também fazer umas perguntas sobre o seu tempo como diretor do NCI Academy. Queria perguntar se considera que essa academia tem tido um efeito positivo a nível nacional na formação de profissionais e na própria formação de pessoas que consigam contribuir para a cibersegurança e para a ciberdefesa em Portugal?

P.V.N. Não se deve ver a escola da NATO, a NCI Academy, que se encontra em Oeiras, como uma propriedade nacional. Não é esse o objetivo.

A.N.A. Sim, sim. Eu sei, mas neste caso era para saber se, como em Portugal... Porque eventualmente tinha mais portugueses a frequentar...

P.V.N. Mas eu explico porquê. Porque o número de pessoas que frequentam essa escola nacional é muito reduzido. É muito reduzido. A escola é, de alguma forma, compartilhada com todos os países da NATO, com todas as estruturas. Portugal é um país dentro dos outros, das nações. Naturalmente tem uma grande vantagem que é o facto da localização geográfica. Não tem custos de deslocação pessoal, etc. Portanto, o rácio de utilização do benefício e reserva de espaço para formar gente é mais favorável a Portugal porque será a "host nation" da escola. Mas este esforço que estamos a falar não se faz pela via da Escola da NATO apenas. Faz-se muito mais pela via daquilo que é uma estratégia nacional. E aí há de facto um quadro que é o quadro de referência de cibersegurança, que o Centro Nacional de Cibersegurança, que de alguma forma tem mobilizado e que foi aprovado e que está na base de um projeto que se chama C Academy que junta escolas, que vai formar gente e que até 2030 tem a ambição de formar 10 mil pessoas em competências na área da cibersecurity.

A.N.A. Sim, eu tinha registrado isso na tese, que era um programa que é "e2030", não é?

P.V.N. Sim, 2030 é a meta que está definida para dar competências às pessoas em cibersecurity.

A.N.A. Sim, sim.

P.V.N. Mas tem de fazer muito mais. Tudo o que se fizer é benéfico e está sempre à queima das necessidades. Portanto, é preciso investir muito.

A.N.A. Há alguns efeitos visíveis na NATO desde que foi fundada a NCI Academy?

P.V.N. Sim, a NATO não tinha um ciber-curriculo. O que nós fizemos, com o nosso projeto, que desenvolvemos no Multinational Cyber Defence Education and Training, foi entregar à escola da NATO o currículo que tínhamos desenvolvido. Eu tive a oportunidade e de alguma forma fui agente dessa passagem, porque a escola antes de estar aqui estava localizada em Latina, em Itália, que era a NATO Communication Information Systems School, depois foi transferida e transformou-se na NATO Communication Information Academy. E aí nós fizemos várias reuniões deste projeto Multinational Cyber Defence Education and Training. Este projeto tinha ao nível da NATO 23 países, uma série de outras organizações, fazendo um total de 40 entidades membros deste projeto.

A.N.A. 23 países?

P.V.N. 23 Países. Tinha países fora da estrutura da NATO, como o Japão, a Macedónia, a Ucrânia, na altura também queria entrar, na União Europeia tinha os países todos da União Europeia, todos os Estados membros. No caso nacional tinha 108 membros, 28 organizações. Universidades, Centros de Investigação, Banca.

A.N.A. 128?

P.V.N. 108. Tinha os stakeholders todos, os ramos das Forças Armadas, o Centro de Cibersegurança e Ciberdefesa. Tinha alguns ministérios, tinha as universidades. Aliás, desse currículo surgiu uma pós-graduação em Cibersegurança e Ciberdefesa, que foi ministrada em conjugação com 11 universidades portuguesas. Em que a Academia Militar exerceu a função de coordenação científica e a Universidade do Minho a coordenação pedagógica, mas que envolveu 11 universidades e que foi feita de uma forma completamente distinta das outras formações anteriores. Normalmente o que é que acontece? Quando há uma formação em ciências clássicas numa universidade, a universidade molda a formação muito à luz daquilo que são as suas competências residentes, os seus professores, os seus centros de investigação, etc. O que nós fizemos foi desenvolver um currículo abstrato, isento, estruturado, com base em determinados pressupostos de formatação dos conteúdos, etc. E depois fomos à procura de onde é que estavam os centros de competências nacionais naquelas áreas. As universidades foram escolhidas porque eram centros de competências naquelas áreas e não porque eram todas elas articuladas em torno dos seus próprios currículos. Mudámos o paradigma completamente. O que resistiu mais a esses esforços? Foi lançado o primeiro curso técnico de cibersegurança, no IEFP, pelo grupo ATEC, da Academia de Formação do grupo Volkswagen. Foi desenvolvido um conjunto de cursos, nomeadamente um curso de decisão estratégica que decorre no IDN, que é feito em colaboração com a Academia Militar, de Gestão de Crise e de Cibersegurança, que tem um exercício final com uma equipa da Estónia, que se ligou connosco desde a primeira edição. Tem um curso de planeamento de operações no ciberespaço que decorre no Instituto Universitário Militar, que todos os anos forma o conjunto de militares para a vida de ciberdefesa, e ajudou a moldar uma série de cursos que fizeram parte agora, todos eles, de um portfólio de um projeto que nasceu na academia militar aqui, que está na sua fase final de edificação, que se chama Cyberacademia Innovation Hub. Este projeto chegou a ser proposto como um headquarters da rede DIANA, que a NATO fundou para financiar startups e componentes de inovador. É relevante.

[END]

Appendix II – Interview Transcript: Rear-Admiral António Gameiro Marques

Appendix II.a – English Translation

[START]

António Gameiro Marques: There are things that emerge from this doctrine that allies, particularly in their military component, must fulfil—or commit to fulfilling. Commitment doesn't necessarily mean compliance, but it implies an obligation to fulfil. Unlike the European Union, which issues directives and/or regulations, directives need to be transposed into national legislation, while regulations come into effect immediately upon application. An example is the eIDAS regulation on Electronic Identification, once enacted and agreed upon by the Member States, it starts functioning through the European Regulation process. However, with a directive, it needs to be transposed. This is not the case in NATO. I worked there for 3 years, and your advisor—aren't they an advisor?—Proença Garcia as well, in similar roles. I was a Navy advisor, and he was an advisor to the Army, to the Ambassador. NATO produces documents and has a rich doctrine. These documents are then approved by the North Atlantic Council, which is the highest body of the Atlantic Alliance and includes all the NATO permanent representatives, who are the ambassadors. Often, there is a NAC at the level of Foreign Affairs or Defence Ministers, and in very exceptional cases, but it happens, there are summits that are NACs at the level of Heads of Government. They are not called NACs, they are called Summits. So, there have been ones in Prague, Lisbon, Warsaw, well, there are several locations, quite significant for the area of cybersecurity and cyber defence within NATO. For example, it was in the Warsaw Summit, if I'm not mistaken, that it was established that cyberspace is another domain of conflict. And therefore, doctrine, procedures, and so on, emanate from there. That's where the subtlety lies. Then, what does NATO do? Just as in the classical components of conflict and war, there is a formal commitment by allies to certain objectives defined by NATO. The same will happen in cybersecurity and cyber defence, if it's not already happening. Is that clear? I'm not sure if I was clear enough.

António Neves Almeida: The first questions here are about how you consider the state of the art of cybersecurity and cyber defence at a general level, at a national level, and at the NATO level?

A.G.M. At the national level, we are following our own path. The primary source of policy and doctrine here at the National Cybersecurity Centre is the European

Union, not NATO. This is because, as I mentioned, the European Union, specifically the European Commission, is prolific in producing directives in this area. The flagship directive is the NIS Directive, which stands for Network and Information Systems Security. It was transposed into our legislation in 2018 through Law 46/2018/13 of August. The regulation of this law was then published in July 2021 through Decree-Law 65/2021 of July 30th. This law, which transposes the directive, is indeed the cornerstone as it establishes the legal framework for cybersecurity. It defines the roles, the central point of authority, the targeted entities, the essential operators, the digital service providers, and so on. As an umbrella for all of this, we have the National Strategy for Cyberspace Security, now in its second version. It is not solely a National Cybersecurity Strategy but deliberately a National Strategy for Cyberspace Security, as it encompasses components of cybersecurity, cyber defence, cyber diplomacy, capacity building in cybersecurity, internal and external relations, cooperation, research, and development. It covers a wide range of security issues in cyberspace. Some countries have chosen to develop a separate National Cybersecurity Strategy. I disagree with this approach unless there is an overarching cyberspace security strategy. I see the National Cybersecurity Strategy as a partial strategy within the broader theme of cyberspace security. It contributes to the National Security Strategy, which Portugal currently does not have. But if it did, that's where it would fit, you see? Recently, as you may be aware, since I have researched this topic, the Cyber Defence Strategy was published. According to the text itself, it aligns and contributes to the national cyberspace strategy, as the former is a general strategy, and the latter is a partial one. Therefore, in Portugal, this strategy, which is entering the revision process, will conclude its cycle in 2023. It will be reformulated and revised because it was created in 2019, and five years is a significant period. Many things have happened in the world between 2019 and 2023.

A.N.A. Especially in cyberspace. When it comes to cyberspace, things change even more rapidly.

A.G.M. Yes, exactly. It's because of technology. Technology undergoes very rapid cycles of change. The Centre, on the other hand, has been in existence for 8 years, reaching its 8th anniversary on October 7th last year. It is making its way. We work within the doctrinal framework derived from the European Union and our own strategy. The NIS Directive 2 (NISS2) is already on the horizon, and it needs to be transposed within 21 months. In other words, we cannot afford to fall behind. This means that by the last quarter, the four-month period of '24, it will have to be transposed. Twelve months from '23, plus ten months from '24, well, not ten, nine. Ideally, it should be incorporated into our legislative framework. As for our interaction with NATO, we primarily engage through the Cyber Defence Centre. They represent Portugal in NATO committees that deal with cyber defence, and as I mentioned earlier, we mainly participate in European Union committees. So, we meet halfway, here, and exchange information through this channel.

A.N.A. The next questions are related to what is lacking in terms of cyberspace, cyber defence, and cybersecurity at the national level.

A.G.M. People. What we lack the most are people.

A.N.A. Both at the national level and within NATO.

A.G.M. Yes. There is a completely different ability to attract and retain talent within NATO compared to the Portuguese public sector. It's not that they don't exist, it's just that I can't retain them for very long. I can't afford to pay the salaries that non-NATO positions or even the private sector in our country can offer. Although we have slightly higher salaries in the national cybersecurity sector compared to the average in the public sector, the private sector is highly competitive and aggressive in terms of compensation. I've been here for almost six years, and every year we see more turnover. That is my biggest challenge. I don't have problems with funding for investment. In the Recovery and Resilience Plan (PRR), we have generous funds for that, but indeed, talent retention is our difficulty.

A.N.A. And at the NATO level, do you have any idea?

A.G.M. At the NATO level, being an alliance and given the current geopolitical situation, they are very exposed to attacks. They have implemented a significant reform in this area in recent years... '20, '22. And as they continue to implement this reform, I am convinced that things will improve significantly. It was mainly an organizational change. NATO is a robust alliance based on the principle of consensus, where all decisions are made through consensus. It has a long history of doctrine. NATO was founded in 1949, so it has many years of experience. Despite the critics of the alliance, without NATO, I don't know what would have happened to Europe.

A.N.A. In your opinion, what do you consider to be the greatest threats, present, current, and future, to the cyberspace?

A.G.M. The greatest threat, in my opinion, is the threat to democratic states. That is the biggest threat because while we often hear about ransomware attacks, sabotage where all information is wiped out, denial of service, and similar things, what will ultimately affect our society the most is the way some states or state-sponsored actors deliberately try to alter our perception of the world. And by doing so, coupled with the fact that we are progressively consuming news less through reliable newspapers and more through social media, we start to see the world through a keyhole with the perspective of those who produce that information. And those who produce it are not certified journalists or professionals. They are individuals influenced by states that aim to distort how

we think and perceive reality. Furthermore, the way we consume information is compromising a fundamental process of democratic states, which is debate. Democracy was born in ancient Greece, where its inventors, the Senate, would debate ideas in the appropriate places. They may not have agreed, but they would discuss them. Today, we still need to know how to debate with respect for the opinions of others, even if they disagree with us. It is through this dialectic process that the best ideas usually emerge. Sadly, I observe, well, sadness is a strong word, but with some discouragement, debates like the ones I had the opportunity to hear during this weekend, such as at the Congress of the Liberal Initiative, right here nearby. Please bear with me. But you see, Antonio, these extreme positions are exacerbated by this consumption of news and our loss of capacity to engage in meaningful debate. This is enabled and amplified by the malicious and detrimental use of cyberspace in society. Therefore, for me, this is the greatest danger. It's the greatest danger because it's like a bacterium that enters our minds and alters our behaviour. Then it creates addictions, dependencies, and we can no longer do without it, and we no longer have time for everything because we also need to eat and take care of ourselves. As a result, there is no time left for what truly makes us useful citizens in a democracy, such as reading a good book, a good article, a good magazine, and engaging in debates. There is no time or patience left for that.

A.N.A. The next question is: how well - or poorly - equipped are we to deal with these threats?

A.G.M. The answer to that question is related not to the previous one but to the one before last. It's a trilogy. And the trilogy is "people, processes, and technology." People need to be structured and organized in a certain way, and this organization is materialized through processes that then use technology to implement them. If we don't have people or enough people, even if we have good processes and are well-organized and have money to buy technology, which we do have, we would still be handicapped because we lack people. How do we mitigate this? I hope... Or at least I have hope. I am convinced that one of the ways to mitigate the lack of people in the future is to use some automated processes. Machines learning how to do things. This would free up people for more unstructured thinking. For more creative thinking. Although machines can be very creative, right? But there needs to be a strong symbiosis between people and machines with that capacity precisely to address this mitigation. Or rather, to mitigate the lack of people in that trilogy: "people, processes, and technology." Is that clear?

A.N.A. And is that the case also within NATO?

A.G.M. Regarding NATO, once again, I doubt it because they are very attractive. In terms of... They manage to attract good human resources, since the school in Oeiras doesn't lack people.

A.N.A. So, in that case, do you think it's also the case for NATO?

A.G.M. In terms of NATO, there is no such problem. The greatest threats to NATO are the fact that the Atlantic Alliance is a political or military alliance, and therefore, its classic detractors will do everything to vectorize attacks perpetrated through cyberspace. That's a certainty. And they do it every day.

A.N.A. The next question, also following up on this last one, is whether you consider NATO, as a superpower, to be somewhat lagging behind compared to China, Russia, and other superpowers?

A.G.M. You see, we can't... China is a sovereign and autocratic state. NATO is an alliance of democratic countries where decisions are made by consensus. There is an abysmal difference right there.

A.N.A. It takes more time.

A.G.M. Much more time. Of course, when a decision is made, it carries a lot of weight, right? Because ultimately, it's a decision that all allies agree on. And it's a very significant bloc. We have the United States of America, Canada, almost all European countries. And now there will be two more, right? Sweden and Finland. Right there, there's a... When no one has to be accountable to anyone to make a decision, even though the government of the People's Republic of China has to resolve matters there, among those 7 people who are the 7 most important leaders, the decision is made and that's it. There's no need to make concessions like in NATO because the document doesn't have to be signed and approved by everyone, it takes many turns. But that's part of Democratic States. Now, we also need to internalize that, despite NATO being based on consensus, those who pay the most have the most say."

A.N.A. The United States.

A.G.M. But it is usually the United States who, even though they pay more, benefit the most in terms of contracts for equipment systems, weapons systems, and the like. For every dollar they invest, they have a significant return for their own country, for their own industry. So, we shouldn't be naive about it.

A.N.A. The next question was also regarding NATO, and it can also be at the national level. To what extent do we, NATO/Portugal, depend on cyberspace for military operations? For day-to-day operations and work within NATO in general?

A.G.M. Nowadays, it is very difficult to imagine scenarios where cyberspace is not available. However, at the operational level, such scenarios do exist. Because if cyberspace... If allies are denied access to cyberspace through a massive attack, a massive denial of service, there could be an alternative in the use of the electromagnetic spectrum. Using non-wired communications. Cyberspace, as defined in our country, which is stated in the early pages of the national cybersecurity strategy, is composed of computer networks, well, I don't know the exact definition, but the dimension of the electromagnetic space, for some authors, is considered cyberspace, while for others it is not. The electromagnetic space, through which we can send data and voice over long distances, even with satellite hops, is crucial. However, the absence or denial of access to cyberspace nowadays has a significant impact on the planning, conduct, and execution of operations. There is no doubt about that. In fact, the most sophisticated aircraft nowadays are always connected to the cloud. The F-35 is a paradigmatic example, and the KC390 that Portugal will receive is the same. They receive the mission, and there are mission operations given in real-time through a cloud to which they are connected.

A.N.A. In your opinion, what importance will cyberspace have in the future?

A.G.M. It will increasingly have more importance because if we look at the emerging technologies that are already being announced and entering full productivity, such as artificial intelligence, digital twins, have you heard of digital twins? A digital twin is when you have a complex physical system, and to better study and understand it in all its aspects, including how to maintain it better, you create a digital twin. A digital twin is a virtual representation of a physical entity. Imagine if instead of having your Mac, you had a digital twin of your Mac. You could fully emulate your Mac without actually having it physically. You would interact with the digital twin through input and output devices like keyboards, mice, and screens, but physically, your laptop wouldn't exist. Then there's the concept of the metaverse, which doesn't exist without cyberspace. All augmented reality, virtual reality, and even from an early age, humans start creating their virtual world. This virtual world then interacts with our physical world through protocols. What are these protocols? It's language, the meaning of things. With the emergence of the digital and cyberspace, the virtual world, which, combined with the physical world, forms the real world, your real world, my real world, has two components that are not of the same size. One component is the tangible aspect of the real world, and the other is the virtual world. The virtual world, with the digital and cyberspace, tends to be much larger than the real world. Why? Because our memories don't exist solely in our biological memory but also in our digital memory. And that's why you may have encountered situations like this: there are people who leave the real world but continue to exist in an extended virtual world through technology. How many people pass away, and Facebook still announces their birthdays... because no one deleted them. And even if they were deleted, the entire history of that person on Instagram, Facebook, LinkedIn, you name it, will endure forever. Do you see?

A.N.A. Yes, yes.

A.G.M. And so, this virtual dimension that a small child who doesn't yet interact, who can barely speak, but is creating around the corners of their everyday life. Then, when they enter the digital world, it's like it's amplified and exponentially increased. And through successive generations, we are better able to deal with this dimension of our lives. Your generation handles it better than mine, and the generation after you will handle it even better because they are almost native to it. They are almost native. Therefore, with metaverses, virtual reality, augmented reality, and with 5G itself, which will allow all of this to be practically omnipresent. Where there is 5G coverage, due to low latency, bandwidth, and speed, what I anticipate is that this symbiotic relationship will only grow. And I believe it will reach its hype, its point of no return when we as humans start becoming bionic. That is, when we start having organs that are constructed using technology. It will happen. Therefore, when we reach that point, where the real world is the sum of the physical and virtual, we begin to question how much of the human body needs to be bionic for a being to be considered bionic and not human. It is born human, born of a mother, the result of a connection between a mother and a father, but over time, it is replaced. I'm delving into science fiction now, you see? But I'm taking us into an abstraction that doesn't seem as fictional given the evolution of technology. Of course, this brings up ethical considerations, but that would lead us down another path.

A.N.A. The next question - in a way, you have already partially answered it - is how significant and damaging the effects of a cyber-attack are today - I recall the case of Iran, the cyber-attack on Iran - and whether you think they will become even more dangerous and impactful in the future?

A.G.M. The cyber-attacks are... What seems evident, and it is already being observed, is that vertical cyber-attacks, that is, attacks that are solely cyber in nature, are impactful. Look at what happened with Vodafone, which was unable to provide services to the majority, the vast majority of its customers for a week, with all the impact it had on both individual customers and businesses, even affecting the emergency hotline 112pt because part of its services relied on Vodafone's infrastructure. However, the most impactful attacks are those that interact with industrial control systems. The example you mentioned earlier in this question is a paradigmatic case of an attack on an industrial control system where the system believed the centrifuges were spinning at the correct speed, but the system was deceiving the controller, and the centrifuges were completely out of control until they reached their physical limit and broke. Now, imagine if it wasn't a centrifuge but a generator in a dam in our country. What would happen if the system that controls, monitors, and commands the energy production through equipment of that magnitude, dimension, and immense inertia went out of control and started breaking? It would result in the dam breaking. What would happen if the system that controls all the signalling of a high-speed train line was hacked and compromised? Those are the situations where we start encountering serious problems. What would happen if the

command-and-control system of a nuclear power plant was compromised and tampered with, endangering the energy production in a nuclear facility? That would indeed result in vertical impacts, a cyber-attack with significant physical consequences. Nowadays, it is observed that cyber-attacks are a component of various mechanisms to attack and achieve a particular purpose. It is what is known as hybrid conflicts, isn't it? You must have come across this concept in your readings. The Helsinki Excellence Centre is a great source of doctrine and has very interesting and good documents on this subject. If you search for it, you will find their website and access some valuable references and documents on this topic.

A.N.A. Regarding the legislative and decision-making side of NATO and Portugal, you mentioned earlier that NATO operates through consensus-based decisions, while other authoritarian countries do not follow the same practice and can advance more rapidly. So, when it comes to legislation and decision-making in NATO countries that are democracies, do they manage to keep up with the evolution of cyberspace?

A.G.M. No, you see, that is a recurring issue where the legislative process, even in autocratic states, is always lagging behind production and innovation. In fact, the aim of regulation is precisely to mitigate technological innovation. Those who develop and innovate are not concerned and do not want to be burdened with regulations and legislation. Usually, there is a reaction, and it is understood that regulation is necessary. In fact, the creation of the internet itself is a good example of this. The internet was born to connect, within the scope of defence, the defence of the United States, as you may know, to connect centres where intercontinental nuclear missiles were located during the Cold War. It started as a relatively controlled movement, but when it later exploded, figuratively speaking, it was meant to promote flexibility, rapid connectivity, easy connection, but it was not designed to be secure. And because it was not designed to be secure, techniques, processes, technology, and human interventions had to be developed and implemented to provide a layer of security. So, even in autocratic countries, I am convinced that legislative production always lags behind technological production, but the gap is much smaller. In autocratic states, if they need to regulate something, they issue a decree, and that's it. Here, it is a legislative process that involves consultations, seeking opinions from all government areas, and then it goes to the Council of Ministers, sometimes it goes back again. If it is a decree-law or a law, it goes to Parliament. With a majority in Parliament, as we have now, it is easier. But it is a time-consuming process. To give you an example, it took us over a year to transpose the NIS Directive, which was published in 2016, not only with the production of legislation but also with its staffing and all the processes associated with consultation and input gathering.

A.N.A. Do you consider that there is any way to streamline this whole process, to avoid taking so much time, especially in the field of cybersecurity, cyberspace?

A.G.M. What seems to me, as we are thinking here and already implementing, is that the law or decree-law should be something generic and framing, and then the more dynamic aspects should be addressed through technical standards produced by the respective authority. This already happens on the INS side. We have legislation that is quite old, from the late 80s, early 90s. But it has the basic principles that regulate the handling of classified information. And then the way we have to adapt is for the National Security Authority to issue technical standards. And it has the legitimacy to do so. These technical standards serve as guidance for those who have to use them. I think it has to be this way because a technical standard needs to have boundaries, it cannot go against the law itself. But it can address procedures and details. And the details, usually, depend on the reality to which they refer. We cannot put such things at the level of law or decree-law. I am an engineer, not a lawyer, but I talk to lawyers here in the organization every day, and throughout my career, I've dealt with international maritime law, administrative law, those kinds of things. And I realized, even by talking to professors from various law faculties, both public and private, that this is a good principle, not to put too much detail in laws or decree-laws, and to reserve that for other pieces that have a dynamic nature, that are more compatible with the dynamics of reality. Otherwise, we are always behind the curve. Always.

A.N.A. The next question is about NATO's strategy, namely whether you think NATO should have a more offensive strategy in its cybersecurity and cyber defence or if it should have a more defensive, passive strategy, or if it should be left to the discretion of each country?

A.G.M. Well, there is some confusion of concepts there. Cybersecurity is not offensive. It is cyber defence that is. Cyber defence, according to the definition, is what allows us, and Brigadier General Viegas Nunes may have explained it to you, to conduct Computer Network Cooperation, operations in the other party's network, whether for exfiltration, exploration, or even attack. Cybersecurity has all the components to protect ourselves, to react to an attack, but not offensively towards others, but to react to an attack in a way that allows us to recover from it. So initially, when the attack happened in Estonia in 2007, I was at NATO at that time, the Allies were very cautious about the offensive capabilities of NATO through cyberspace. It was only later that it started to appear in the doctrine. So, these Computer Network Cooperations now exist, as far as I know, in NATO's doctrine. But NATO does or will do it when its own facilities, infrastructure, or commands are attacked. Or NATO forces. And NATO forces are those provided by the countries. The doctrine provides for that, but the use of force even through cyberspace is something that has to be legitimately sanctioned by the NAC and the Military Committee. Below the NAC, there is the Military Committee, which brings together all the Chiefs of Defence of the Allies.

A.N.A. I only mentioned the offensive part of cybersecurity because I read that countries like the United Kingdom and the United States have an offensive strategy, meaning they are not waiting to be attacked but are actively 'attacking' adversaries to prevent them from having the opportunity to attack these countries.

A.G.M. Once you have the capability, you can engage in pre-emption, which is what you are saying, attacking before being attacked. When in doubt, you receive a straight punch to keep you still, which, by the way, was the doctrine of the United States of America during the time of Hussein with Bush. There are countries that have the capacity to develop and use cyber weapons, and that's what they do if they are attacked, with the legitimate endorsement of their governments. Then there are countries that don't have that capability. NATO will openly use these means only if authorized by the NAC. I'm not saying it won't happen.

A.N.A. The penultimate question is whether NATO should implement a unified cybersecurity strategy and have it implemented within the Alliance among its member states, or if it should be left to the discretion of each country?

A.G.M. Let's separate two things here. One thing is NATO's strategy for its commands, its facilities. It has that. Another thing is what each Member State should do. And there, it binds through commitments and planning, like all allies do in the Air Force, Army, and Navy, but now also in the cyber dimension because it is also a potential dimension of conflict, like space. Therefore, what NATO intends is to have some balance, some harmony, so that there is no state that is very weak in this area, and then another state... And if that state is attacked and becomes vulnerable, it weakens the alliance. NATO is not a state. NATO is an alliance of a group of allies that have common objectives and ways of engaging with the world and a set of rules, which are outlined in the North Atlantic Treaty, that govern all interaction between allies. Now, while the European Union creates regulations that all Member States must comply with, such as the General Data Protection Regulation, the Atlantic Alliance cannot do that. It does not create doctrines that all allies must comply with. No. There is then the process of force planning, in which states commit to what they commit to. And then there is a negotiation process, and at the end of that cycle, an examination is conducted to verify whether the commitments made by the states have been achieved or not. And it goes on like that.

A.N.A. My last question is whether you consider that this NATO school here in Portugal has had any visible effect on NATO's cyber capabilities?

A.G.M. They are working at... Not only at a steady pace but also with a vision for the future that, in my opinion, is and will continue to be a game-changer for NATO in this area. Of course, at this moment, that school, which aims to be a true academy, the 'NATO Communication and Information Academy,' wants to

offer academic courses and conduct research, but it is not able to do so yet. Currently, they are providing a lot of training on existing systems due to the conflict in Ukraine. However, the school director's vision is oriented in that direction. Not only to continue offering the courses they currently provide but also to establish a more formal approach. To look beyond the horizon.

[END]

[START]

António Gameiro Marques: Há coisas que emergem dessa doutrina que os aliados, designadamente na sua componente militar, devem, ou comprometem-se a cumprir - comprometem-se, não significa que cumpram, mas comprometem a cumprir. Contrariamente à União Europeia, a União Europeia, como sabe, emite diretivas e/ou regulamentos. As diretivas depois têm de ser transpostas para a legislação nacional e os regulamentos entram logo em funcionamento, em aplicação. Um exemplo é o regulamento do eIDAS, da Identificação Eletrónica, uma vez promulgado e acordado pelos Estados Membros, a tramitação pelo Regulamento Europeu, os Estados Membros, etc., passa a funcionar. Numa diretiva, não, tem que ser transposta. Na NATO não é assim. Eu trabalhei lá há 3 anos, e o seu orientador - não é orientador? - Proença Garcia também, precisamente em funções semelhantes, eu era conselheiro de Marinha, e ele conselheiro do Exército, do Sr. Embaixador. A NATO, produz documentos, é muito rica em doutrina. Esses documentos depois são aprovados pelo North Atlantic Council, que é o órgão máximo da Aliança Atlântica, onde estão representados todos os representantes permanentes da NATO, são os embaixadores, e muitas vezes há um NAC ao nível de Ministro de Negócios Estrangeiros ou Ministro da Defesa, e em casos muito excecionais, mas ocorre, pelo menos há as cimeiras que são NACs ao nível de chefes de Governo, não se chamam NACs, chamam Cimeiras. E, portanto, há de Praga, houve de Lisboa, de Varsóvia, enfim, há várias comarcos, aliás, bastante significativos para a área da cibersegurança e ciberdefesa no NATO. Por exemplo, é na de - salvo erro- Varsóvia que se estabeleceu que o ciberespaço é mais um domínio de conflito. E, portanto, isso depois é daí que emana doutrina, procedimentos, etc. Por isso há aí uma subtileza. Depois, o que é que a NATO faz? Tal como nas componentes clássicas do conflito e da guerra há um comprometimento formal dos aliados perante determinados objetivos, que a NATO define, na cibersegurança e na ciberdefesa também vai passar a haver, se é que já não está a haver. Está bem? Não sei se foi claro.

António Neves Almeida: As primeiras perguntas aqui são sobre como é que considera o estado da arte de cibersegurança e ciberdefesa a nível geral, a nível nacional e a nível da NATO?

A.G.M. A nível nacional nós estamos a percorrer o nosso caminho, a nossa fonte de política, de doutrina, primordial aqui no Centro Nacional de Cibersegurança é a União Europeia e não a NATO. Até porque, como eu disse, a União Europeia, concretamente a Comissão Europeia, que profícua na produção de

diretivas sobre esta área, sendo que aquela que é, digamos, a bandeira é a diretiva NISS, Network and Information Systems Security. Ela foi transposta para a nossa legislação em 2018, na Lei 46/2018/13 de Agosto, e depois a regulamentação dessa lei foi publicada em Julho de 2021, através do Decreto-Lei 65/2021, de 30 de Julho, e esta lei que transpõe a Diretiva é de facto o pilar porque estabelece o regime jurídico de segurança do ciberespaço. Quem é quem, quem é o ponto único, quem é a autoridade, quem é que são as entidades visadas, os operadores essenciais, os prestadores digitais, está lá tudo. Como "umbrella" disto tudo, há a Estratégia Nacional de Segurança do Ciberespaço, já na sua segunda versão. Não é uma Estratégia Nacional de Cibersegurança, é premeditadamente uma Estratégia Nacional de Segurança do Ciberespaço, porque engloba componentes de cibersegurança, mas também engloba componentes de ciberdefesa, engloba ciberdiplomacia, capacitação em cibersegurança, relações externas e internas, cooperação, investigação e desenvolvimento, tem uma... Contempla a temática de segurança no ciberespaço em diversos componentes, ampla. Há países que optaram por fazer uma estratégia nacional de cibersegurança. Eu não concordo com essa abordagem, a não ser que haja uma de segurança do ciberespaço por cima. Eu vejo a Estratégia Nacional de cibersegurança como uma estratégia parcial da temática mais lata que é a segurança do ciberespaço. Que contribui depois para a Estratégia de Segurança Nacional que Portugal não tem. Mas se tivesse, era aí que se encaixaria, está a ver? Recentemente, como saberá, até porque investiguei esse tema, foi publicada a Estratégia de Ciberdefesa, que, como diz o próprio texto, alinha, é um contributor, um contributo, alinha com a estratégia nacional de ciberespaço, porque esta é uma estratégia geral e não uma parcial, como é a de Ciberdefesa. Portanto, em Portugal, esta estratégia que está a entrar no processo de revisão termina este ciclo de 2023. Portanto, vai ser reformulada, vai ser revista, porque ela é de '19. 5 anos é muito ano. Passou-se muita coisa no mundo entre '19 e '23.

A.N.A. Especialmente no ciberespaço. Quanto ao ciberespaço, as coisas mudam ainda mais rápido.

A.G.M. Sim, exatamente. Porque é o decorre da tecnologia. A tecnologia tem ciclos de mudança muito rápidos. O Centro em contrapartida existe há 8 anos, que fez em 7 de outubro do ano passado 8 anos. Está a fazer o seu caminho. Nós trabalhamos muito enquadrados neste edifício doutrinário que decorre da União Europeia e da nossa estratégia. Já está a vir a NISS2, que tem de ser transposta para além em 21 meses. Ou seja, nós não nos podemos atrasar, o que significa que algures no último trimestre, o quadrimestre de '24, terá que ser transposta, 12 meses de '23, mais 10 meses de '24, 10 não, 9, ela terá que estar vertida desejavelmente na nossa matriz legislativa. Nós, como é que interagimos com a NATO? Interagimos com a NATO, sobretudo através do Centro de Ciberdefesa. São eles que representam Portugal nos comités da NATO que tratam o assunto de ciberdefesa, "ciberdefence", e nós vamos sobretudo a comités da União Europeia com o já lhe disse. E, portanto, depois encontramo-nos a meio, ou seja, aqui, e trocamos a informação por aqui.

A.N.A. As próximas perguntas têm a ver com o que está em falta a nível de ciberespaço, ciberdefesa, cibersegurança, em termos nacionais.

A.G.M. Pessoas. O que mais falta são pessoas.

A.N.A. Na nacional e também na NATO.

A.G.M. Sim. Há uma capacidade de captar e reter talento na NATO completamente diferente do que existe no setor público português. Não é que eles não existam, só que eu não consigo retê-los muito tempo. Eu não consigo pagar os salários que hoje em dia que não são NATO, mas também o setor privado do nosso país consegue. Apesar de nós termos salários um pouquinho acima, nós, o setor nacional de Cibersegurança, um pouquinho acima da média do setor público, mas o mercado, o setor privado está muito competitivo, muito agressivo, agressivo no sentido figurado do tempo e eu já cá estou há seis anos, quase seis meses, e todos os anos roda mais gente. Essa é a minha maior dificuldade. Não tenho problemas de dinheiro para investimento. No PRR temos verbas bastante generosas para isso, mas de facto essa é a nossa dificuldade.

A.N.A. E a nível da NATO tem alguma ideia?

A.G.M. A nível da NATO, eles são numa aliança, inclusive com a atual situação geopolítica, muito exposta a ataques. E eles fizeram uma reforma nesta área muito profunda com os últimos... '20, '22. E quando implementar essa forma, e estão a implementá-la, estou convencido que as coisas ficarão bastante melhor. Era mais a nível organizacional. A NATO é uma aliança muito robusta porque assenta, no princípio do consenso, todas as decisões são tomadas em consenso. E tem um historial enorme de doutrina. A NATO foi fundada em 1949. Portanto, tem muitos anos já de vida glútea, e apesar de muitos detratores da aliança, não fora ela eu não sei o que teria acontecido já à Europa.

A.N.A. Na sua opinião, qual é que considera que são as maiores ameaças, presentes, atuais, e futuras para o ciberespaço?

A.G.M. As maiores ameaças para mim são as ameaças aos estados de direto democrático. Essa é a maior ameaça porque enquanto aquilo que mais ouvimos falar são ataques de ransomware e de sabotagem onde apagam a informação toda. E "denial of service" e esse tipo de coisas. E até espionagem e desfiltração de informação. Aquilo que mais nos virá afetar enquanto a sociedade é a forma como também alguns Estados ou States Sponsored Actors, premeditadamente, tentam todos os dias alterar a forma como nós percecionamos o mundo. E ao fazer isso, associado ao facto de que nós estamos progressivamente a deixar de consumir notícias através de jornais fide dignos, a ouvir notícias com diversas perspetivas editoriais e consumimos informação, seja ela de que qualidade for, através de redes sociais, passamos a ver o mundo por um buraquinho da fechadura, com a perspetiva de quem produz aquilo. E quem produz aquilo não é um jornalista encartado, não é um jornalista profissional. São pessoas que são assolo de Estados que têm como objetivo deturpar a forma como nós pensamos e percecionamos a realidade. Mais, essa forma como consumimos informação está a comprometer um processo fundamental dos Estados Democráticos, que é o debate. A democracia nasce na Grécia clássica onde os seus inventores, o Senado, nos sítios próprios debatiam as ideias, podiam não estar de acordo, mas

debatiam-nas e hoje nós temos que continuar a saber debatê-las com respeito pela opinião do outro, mesmo que o outro não concorde connosco. E é dessa dialética que normalmente saem as melhores ideias. E eu vejo com tristeza, enfim, com tristeza é muito forte, mas com algum desanimo, debates, como ontem tive oportunidade, durante este fim de semana, de ouvir, em alguns casos, do Congresso da Iniciativa Liberal, aqui mesmo, pertinho. Peço a paciência. Mas está a ver, António, estas posições extremadas são exacerbadas por esse consumo de notícias e por essa incapacidade que nós temos, por a perda dessa capacidade. E isso é "enabled" e potenciado pelo uso do ciberespaço de forma perniciosa e má para a sociedade. Portanto, para mim, esse é o maior perigo. É o maior perigo porque isso é como se fosse uma bactéria que entra na nossa cabeça e que modifica o nosso comportamento. E depois cria vícios, cria "addiction" e nós já não conseguimos passar sem isso e não temos tempo para tudo, porque também temos que comer e alimentarmo-nos. E, portanto, depois não sobra tempo para aquilo que efetivamente nos faz cidadãos úteis para a democracia. Ler um bom livro, um bom artigo, uma boa revista, debater isso, não dá tempo para isso, nem paciência.

A.N.A. A próxima pergunta é: quão bem - ou mal - equipados estamos para lidar com essas ameaças?

A.G.M. A resposta a essa pergunta está relacionada, não com a anterior, mas com a penúltima. Que é, tudo isto é resultado de uma trilogia. E a trilogia é "pessoas, processos e tecnologia". As pessoas têm de estar estruturadas e organizadas de certa maneira e essa organização é consubstanciada nos processos que depois usam a tecnologia para os concretizar. Se não temos pessoas ou pessoas suficientes, mesmo que tivéssemos bons processos e fôssemos bem organizados e tivéssemos dinheiro para comprar tecnologia, que até temos, ficaríamos sempre coxos. Porque não temos pessoas. Como é que se mitiga isso? Eu tenho esperança que... Ou pelo menos tenho esperança. Estou convencido que uma das formas que no futuro poderá haver para mitigar a falta das pessoas é usar alguns processos automatizados. Através de... As máquinas a aprenderem como têm que fazer aquilo. Para libertar as pessoas para pensamento mais... Não estruturado. Para pensamento mais criativo. Embora as máquinas possam ser muito criativas, não é? Mas tem que haver aqui uma simbiose muito grande entre as pessoas e as máquinas dotadas dessa capacidade para, precisamente, fazer face a essa mitigação. Ou melhor, para mitigar essa falta de pessoas na tal trilogia: "pessoas processos e tecnológica". Está bem?

A.N.A. E isso a nível também da NATO?

A.G.M. Da NATO, eu, mais uma vez, duvido porque eles são muito atrativos. Em termos de... Eles conseguem atrair bom recursos humanos, já que a escola em Oeiras, não tem falta de gente.

A.N.A. Portanto, nesse caso, acha que é também em termos da NATO?

A.G.M. Em termos da NATO não há esse problema. As maiores ameaças à NATO é o facto de a Aliança Atlântica ser uma aliança política ou militar e, portanto, os seus detratores clássicos tudo farão para vetorizar com ataques

perpetrados através do ciberespaço. Nisso, certeza absoluta. E fazem todos os dias.

A.N.A. A próxima pergunta, também no seguimento desta última, é se considera que a NATO, como superpoder, está de alguma forma atrasada, comparado com a China, a Rússia e outros superpoderes?

A.G.M. Veja, não podemos... A China é um Estado soberano e autocrático. A NATO é uma aliança de países democráticos, onde a decisão é tomada em consenso. Logo aí, há uma diferença abissal.

A.N.A. Demora mais tempo.

A.G.M. Muito mais tempo. Claro que a decisão quando é tomada tem muita força, não é? Porque, no fundo, é uma decisão que todos os aliados concordam. E é um bloco muito significativo. Temos os Estados Unidos da América, tem o Canadá, temos países europeus quase todos. E agora vai ter mais dois, não é? A Suécia e a Finlândia. Logo aí há uma... Quando ninguém tem que dar conta a ninguém para tomar decisão, mesmo que o governo da República Popular da China tenha que dirimir os assuntos lá, no meio daquelas 7 pessoas que são os 7 governantes mais importantes, tomou a decisão e acabou. Não tem que andar a fazer concessões como se tem que fazer na NATO porque o documento não tem a ser assinado por todos e aprovado por todos, leva muitas voltas. Mas isso faz parte dos Estados Democráticos. Agora, também precisamos de nos interiorizar que, apesar de a NATO ser em consenso, quem mais manda na NATO é quem mais paga.

A.N.A. Os Estados Unidos.

A.G.M. Mas também são normalmente os Estados Unidos que, ainda que mais paguem, são quem mais usufruem em termos de contrato, de contratos para sistemas de equipamentos, sistemas de armas com equipamentos e afins. Por cada dólar que eles metem têm um retorno significativo para o seu próprio país, para a sua própria indústria. Então não convém que sejamos naïves.

A.N.A. A próxima pergunta era também a nível da NATO, e também pode ser a nível nacional também. A que nível é que nós, NATO/Portugal, dependemos do ciberespaço para operações militares? Para o dia-a-dia de operações, de trabalho em geral da NATO?

A.G.M. Hoje em dia é muito difícil conceder cenários em que o ciberespaço não está disponível. Todavia, ao nível operacional, esses cenários existem. Porque depois, se o ciberespaço... For negado o acesso aos aliados, ao ciberespaço, com um ataque massivo, o maciço de "denial of service", negação do acesso, poderá haver a alternativa da utilização do espectro eletromagnético. Usar comunicações não-filares. O ciberespaço, pela definição que nós adotámos no nosso país, que está logo nas primeiras páginas da estratégia nacional de segurança do ciberespaço, é constituído pela rede de computadores, enfim, não sei a definição de cor, mas a dimensão do espaço eletromagnético, para alguns autores é a considerado ciberespaço, para outros não é. O espaço

eletromagnético, através do qual podemos enviar dados e voz a distâncias grandes, até com saltos satélite, é fundamental. Agora, a inexistência ou a negação do acesso ao ciberespaço tem hoje em dia, um impacto muito significativo no planeamento, condução e condução das operações. Isso não há dúvida nenhuma. Aliás, as aeronaves mais sofisticadas hoje em dia estão sempre ligadas à nuvem. O F-35 é um caso paradigmático, o KC390 que Portugal vai receber a mesma coisa. Recebe a missão e há operações dadas à missão no tempo real, através de uma cloud a que eles estão ligados.

A.N.A. Na sua opinião, qual é a importância que o ciberespaço vai ter no futuro?

A.G.M. Cada vez vai ter mais importância, porque veja: só as tecnologias emergentes que já se anunciam e que já estão a entrar em "produtiva em pleno", como as inteligências artificiais, os digital twins, já ouviu falar dos digital twins? O digital twin é: imagine que tem um sistema complexo físico, e para o estudar melhor, e para, em todas as suas vertentes, para perceber como é que o pode manter melhor, manter na manutenção, faz um digital twin. Um digital twin é um digital twin do motor elétrico, é um motor elétrico virtual. O digital twin de um gerador é algo que é a representação lógica daquela entidade física. Imagine que você, em vez de ter o seu Mac, tinha um digital twin do Mac, podia emular na plenitude o seu Mac sem ter o seu Mac. Tinha o seu Mac apenas na dimensão virtual, mas usável através de dispositivos de entrada e de saída, teclados, ratos e ecrãs, mas fisicamente o seu portátil não existia, você interagia com o Digital Twin. Depois há a questão do metaverso, que o metaverso sem o ciberespaço não existe. Toda a realidade aumentada, toda a realidade virtual, e, portanto, nós - e uma vez ouvi falar nisto e acho que nunca mais me vou esquecer pelo menos até não ter memória - nós seres humanos quando nascemos começamos a criar o modelo mental das coisas. Portanto, começamos a criar o nosso mundo virtual sem interagir com o digital. Nós desde pequenos começamos a criar o nosso mundo virtual. Que interage depois com o nosso mundo físico através de protocolos. E quais são os protocolos? É a língua, é o significado das coisas. Com a emergência do digital e do ciberespaço, o mundo virtual que, com o mundo físico, forma o mundo real, o seu mundo real, o meu mundo real, tem duas componentes que não são, que não têm o mesmo tamanho. Uma componente do mundo real, do tangível, e do mundo virtual. E o mundo virtual com digital e ciberespaço, tem tendência a ser muito maior do que o mundo real. Porquê? Porque quanto mais não o seja, porque as nossas memórias não existem só na nossa memória biológica, mas também existem na nossa memória ou na memória digital. E é por isso que - e você já se deve ter confrontado com situações destas que vou descrever - há pessoas que deixam o mundo real e continuam a existir num mundo virtual estendido através da tecnologia. Quantas pessoas é que falecem e continua o Facebook a dizer que elas... Faz anos no dia tal... Porque ninguém apagou. E mesmo que apagassem, todo o historial daquela pessoa no Instagram, no Facebook, no LinkedIn, you name it, perdurará para sempre. Está a ver?

A.N.A. Sim, sim.

A.G.M. E, portanto, essa dimensão virtual que uma criança pequenina que ainda não interage, mal sabe falar, mas que vai criando à volta dos esquinos que

compõe a vida dela todos os dias. Depois, quando chega ao digital, isso é como se fosse amplificado, exponenciado brutalmente. E nós, por sucessivas gerações, vamos conseguindo lidar com essa dimensão da nossa vida muito melhor. A sua geração lida melhor com isso do que a minha e a geração a seguir a si há de lidar melhor ainda porque já é quase nativo. Já é quase nativo. Por isso, então com os metaversos, com a realidade virtual, com a realidade aumentada, com o próprio 5G que vai permitir que tudo isso esteja praticamente omnipresente. Onde haja cobertura 5G, por causa da baixa latência, por causa da largura de bando e da rapidez e dessas coisas todas, o que eu antecipo é que essa simbiose, essa relação simbiótica cada vez seja maior. E acho q vai ter o seu hype, o seu ponto de completo não retorno quando nós, seres humanos, começarmos a ser biónicos. Ou seja, começarmos a ter órgãos que são construídos a partir da tecnologia. Isso há de acontecer. Vai acontecer. E por isso, aí, enquanto que o mundo real é no somatório do físico ou virtual, depois começa a se perguntar quanto é que é preciso o corpo humano ser biónico para que o ser seja um ser biónico e não seja um ser humano. Nasce humano. Nasce de uma mãe, fruto de uma ligação entre uma mãe e um pai, mas ao longo da vida é substituído. Já estou a fazer ficção científica, percebe? Mas estou a levar-nos para uma abstração que, enfim, não me parece que seja tão ficção como isso em face da evolução da tecnologia. Claro que aqui depois começam-se a colocar situações que todos os dias nos assistem que são as situações da ética. Mas isso entrávamos por outro caminho.

A.N.A. A próxima pergunta - de certo modo já chegou a responder mais ou menos a isto - Quão grande são os efeitos, quão damaging são os efeitos de um ciber-ataque hoje - lembro-me do caso do Irão, o ciber-ataque ao Irão - e se acha que no futuro vão ser ainda mais perigosos, mais impactantes?

A.G.M. Os ciberataques são... O que me parece, e já se está a verificar, é que os ciberataques verticais, ou seja, que são só ciberataques, são impactantes, veja o que aconteceu com o Vodafone, que ficou sem providenciar serviços a maioria, a grande maioria dos seus serviços durante uma semana, com todo o impacto que teve em todos os seus clientes, quer os clientes singulares, quer as empresas, e até o 112pt que foi afetado, porque parte dos seus serviços estava na infraestrutura da Vodafone. Mas os mais impactantes, hão de ser aqueles, e já são, aqueles que interagem com sistemas de controle industrial. O exemplo que deu logo a princípio desta pergunta é um caso paradigmático de um ataque que foi feito a um sistema de controle industrial em que o sistema pensava que a centrifugadoras estavam a rodar à velocidade certa e o sistema estava a enganar o controlador e as centrifugadoras estavam completamente desarvoradas até que atingiram o seu limite físico e partiram. Agora, imagine que aquilo não era uma centrifugadora, mas era um gerador numa qualquer barragem no nosso país. O que é que aconteceria se o sistema que controla e monitoriza e comanda a produção de energia através de equipamentos daquela tonelagem, daquela dimensão e daquela inércia gigantesca, desarvorasse e começasse a partir? E o partia-se a barragem. O que aconteceria se o sistema que controla toda a sinalética de uma linha de alta velocidade de comboio, fosse hacked e comprometido. Isso aí é que começam a ser problemas graves. O que aconteceria se o sistema de comando e controle de uma central nuclear fosse comprometido e interferido de maneira a pôr em perigo a produção de energia

numa central nuclear. Aí sim, iríamos ter impactos verticais, era um ciberataque com impactos físicos muito grandes. Hoje em dia o que se verifica é que os ciberataques são uma componente de vários outros mecanismos para atacar e para atingir um determinado propósito. É o que se chama, os conflitos de natureza híbrida, não é? Você já deve ter tropeçado, digamos assim, na sua leitura que tem feito. O Centro de Excelência em Helsinquia é uma grande fonte de doutrina, tem documentos muito interessantes e muito bons sobre essa temática. Se você fizer uma procura, vai lá ter ao site, se precisar de bibliografia e de documentos interessantes sobre esse assunto.

A.N.A. Haver mais com o lado legislativo, de decision making da NATO e também de Portugal, aliás, porque tocou há bocado nesse ponto sobre a NATO funcionar através de decisões consensuais e outros países, sendo autoritários, não terem a mesma prática, portanto, avançam mais rapidamente, se a legislação, se o decision making da NATO, em países democráticos que integram a NATO, conseguem "keep up" com a evolução do ciberespaço?

A.G.M. Não, veja, isso é um assunto recorrente que o processo legislativo, até mesmo nos Estados autocráticos, está sempre "lagging" a produção e a inovação. Aliás, o que é que se tenta fazer com a regulação? É fazer precisamente o amortecimento da inovação tecnológica. Quem desenvolve, quem quer inovar, não se está preocupado e nem quer estar preocupado com regulamentação e com legislação. Normalmente há uma reação. Pois é isso, porque se percebe que tem que se regular. Aliás, a criação da própria internet é disso também um caso como um bom exemplo. A internet nasce para ligar, nasce no âmbito da defesa, da defesa dos Estados Unidos, como você saberá, para ligar centrais, no caso da Guerra Fria, centrais onde estavam mísseis intercontinentais nucleares. Nasce um movimento relativamente controlado, mas quando depois explode, e explode no sentido figurado do termo obviamente, nasce para promover, para ser flexível, rápida, facilmente conectável, não foi pensada para ser segura. E como não foi pensada para ser segura, então teve que se começar a pensar e a implementar técnicas e processos, tecnologia e processos com as pessoas para lhe darem uma camada de segurança. Por isso, mesmo os países autocráticos estou convencido que a produção legislativa está sempre atrás da produção tecnológica, no entanto o gap é muito menor. Porque no Estado autocrático se é preciso regular aqui, fazem um despacho e pronto. Aqui não, é um processo legislativo, anda às voltas, tem que perguntar. Na NATO é consenso. Aqui, nos Estados democráticos, nós temos um processo legislativo, quando alguém faz uma lei tem que a submeter, ela vai ao parecer de todas as áreas governativas, depois vai a Conselho de Ministros, às vezes volta outra vez para trás. Se é um decreto de lei, se for uma lei é no Parlamento. Com o Parlamento de maioria, como temos agora, é mais fácil. Mas é um processo moroso. Para dizer, nós para fazermos a transposição da Diretiva NISS, que foi publicada em 2016, nós andamos mais de um ano nesta, não só com a produção da legislação, mas depois com o seu staffing, com todos os processos associados à consulta e à introdução de contributos.

A.N.A. E considera que há alguma maneira de dinamizar esse processo todo, para não demorar tanto tempo, principalmente na área de cibersegurança, ciberespaço?

A.G.M. O que me parece, nós estamos aqui a pensar e já estamos a implementar, é haver a lei ou decreto de lei ser algo genérico e enquadrador e depois o que é mais dinâmico serem normas técnicas que são produzidas pela autoridade respetiva. Isso já acontece no lado do INS. Nós temos uma legislação que tem é bastante antiga, é da década... Fins da década de 80, princípio da década de 90. Mas ela tem os princípios básicos que regulam a tramitação da informação classificada. E depois a maneira de nós termos de nos adaptarmos é a autoridade nacional de segurança promulga normas técnicas. E tem legitimidade para o fazer. E as normas técnicas servem de guidance a quem tem que usar aquilo. Acho que tem de ser assim porque uma norma técnica tem que ter baias, não pode ir contra a própria lei que há ali. Mas já vai aos procedimentos, já vai ao detalhe. E o detalhe, normalmente, é a função da realidade a que ele se refere. Não podemos pôr coisas dessas ao nível da lei ou do decreto de lei. Eu sou engenheiro, não sou jurista, mas falo todos os dias com juristas aqui da casa e ao longo da minha carreira tive direito de internacional marítimo, direito administrativo, essas coisas. E percebi, até por falar com professores de diversas faculdades de direito, quer públicas, quer privadas, que este é um bom princípio, não pôr demasiado detalhe nas leis ou nos decretos de leis, e reservar isso para outras peças que tenham uma dinâmica, que sejam mais compagináveis com a dinâmica da realidade. Porque senão estamos sempre atrás do prejuízo. Sempre.

A.N.A. A próxima pergunta tem a ver com a estratégia da NATO, ou seja, se acha que a NATO deve ter uma estratégia mais ofensiva na sua cibersegurança, ciberdefesa, ou se deve ter uma estratégia mais defensiva, mais passiva ou deve-se deixar isso ao critério de cada país?

A.G.M. Bom, há aí uma confusão de conceitos. A cibersegurança não é ofensiva. A ciberdefesa é que é. A ciberdefesa, segundo a definição, é aquilo que nos permite, e o Brigadeiro-General Viegas Nunes é capaz de lhe ter explicando isso, é aquilo que nos permite fazer Computer Network Cooperation, operações na rede do outro, quer de exfiltração, quer de exploração, quer mesmo de ataque. A cibersegurança tem as características, tem todas as componentes para nos protegermos, para reagirmos a um ataque, mas não ofensivamente ao outro, mas reagirmos a um ataque, de maneira a que conseguimos recuperar desse ataque. Portanto, ao princípio, eu estava na NATO nessa altura, quando foi o ataque na Estónia, em 2007, os aliados foram muito cautelosos na capacidade ofensiva da NATO através do ciberespaço. Só depois é que isso começou a aparecer na doutrina. Portanto, as tais Computer Natural Corporation, elas agora já existem, que eu saiba, na doutrina da NATO. Mas a NATO faz isso ou fará isso quando as suas próprias instalações ou infraestruturas ou comandos forem atacados. Ou forças da NATO. E as forças da NATO são aquelas que são providenciadas pelos países. A doutrina prevê isso, mas a utilização da força mesmo através do ciberespaço é algo que tem que ser sancionado legitimamente pelo NAC e pelo Comité Militar. A baixo do NAC está o Comité Militar que reúne todos os CEMFAS dos aliados.

A.N.A. Eu só disse isso, que era a parte ofensiva da cibersegurança porque eu li que países como o Reino Unido e os Estados Unidos, têm uma estratégia ofensiva, ou seja, não estão à espera de ser atacados, vão "atacando" os adversários para não haver abertura nem oportunidade desses adversários atacarem esses países.

A.G.M. Depois de se ter a capacidade, pode se fazer uma preemption, que é o que você está a dizer, eles atacam antes de serem atacados. Em caso de dúvida, levas com uma reta que é para te pores quieto, que aliás era a doutrina dos Estados Unidos da América, no tempo do Hussein, com o Bush. Há países que têm essa capacidade de fabricar e de usar armas cibernéticas, é o que fazem se forem atacados, com o legitimo endorsement dos governos, os países. Depois há os países que não têm essa capacidade. A NATO só abertamente utilizará esses meios se o NAC autorizar. Não digo que não faça.

A.N.A. A penúltima pergunta é se a NATO deve implementar uma estratégia única de segurança no ciber espaço, e ter isso implementado na Aliança, entre os seus estados-membros, ou se deve deixar ao critério de cada país?

A.G.M. Vamos separar aqui duas coisas. Uma coisa é a estratégia da NATO para os seus comandos, as suas instalações. Isso ela tem. Outra coisa é aquilo que cada Estado Membro deverá fazer. E aí faz esse “binding” através dos tais compromissos e planeamento, como todos os aliados; que há nas Forças Aéreas, Terrestres e navais, mas também existe agora na dimensão ciber, por causa de ser também uma dimensão possível de conflito como o espaço. Portanto, o que a NATO pretende é que haja algum equilíbrio, alguma harmonia, para não haver um Estado que é muito debilitado nessa área e depois outro... E esse Estado depois é atacado e se for atacado fragiliza a aliança. A NATO não é um Estado. A NATO é uma aliança de um conjunto de aliados que têm determinados objetivos e maneiras de estar no mundo comuns e que têm um conjunto de regras, que estão no tratado do Atlantico Norte, que regem toda a interação entre os aliados. Agora, enquanto que a União Europeia faz regulamentos e todos os Estados Membros têm que cumprir, como o regulamento geral de proteção de dados pessoais, a Aliança Atlântica não consegue fazer isso. Não faz isso. Não faz doutrina que depois todos os aliados têm de cumprir. Não. Há depois o tal processo de "force planning", de planeamento de forças, em que os Estados se comprometem a fazer aquilo a que se comprometem. E depois há um processo negocial e depois há um exame ao fim desse ciclo para verificar se aquilo que os Estados comprometeram foi atingido ou não foi. E vai se fazendo assim.

A.N.A. A minha última pergunta é se considera que esta escola da NATO aqui em Portugal tem tido algum efeito visível nas capacidades ciber da NATO?

A.G.M. Eles estão com... Não só com um ritmo, mas também com uma visão para o futuro, que me parece que vai ser... Já é e vai continuar a ser e ainda será mais um "game changer" da NATO nesta área. Claro que, neste momento, aquela escola que quer ser uma academia de facto, "NATO Communication and Information Academy", quer dar cursos académicos, quer fazer investigação e hoje ainda não consegue fazer isso. Hoje estão a dar muita formação em sistemas existentes por causa do conflito da Ucrânia. Mas a visão do diretor da

escola é nesse sentido. Não só continuar a dar os cursos que dá, mas também fazer um "formal looking". Olhar para lá do horizonte.

[END]

Appendix III – Interview Transcript: Coordinator Lino Santos

Appendix III.a – English Translation

[START]

António Neves Almeida: First question I had was: what is your view on the current state of the art of cybersecurity in a general aspect, a national aspect, and eventually in the NATO aspect?

Lino Santos: State of the art in cybersecurity. This depends more on the definition of cybersecurity, which is not exactly consensual. But I must say that I think there are three factors that contribute to a high societal vulnerability. The first factor relates to a highly sophisticated threat landscape, ranging from state actors, cybercriminals, organized cybercrime, to activists. There is a convergence between hacking techniques and political activism, as well as non-politically motivated individuals, including young individuals who engage in illicit cyber activities for challenges or peer recognition. It is a complex threat landscape where it is difficult to effectively attribute responsibilities, given the blurred boundaries between these actors. We have some concrete examples, from false flag attacks to cyber militias like the Killnet group. On the Ukrainian side, there are similar groups carrying out attacks with the consent of the governments of the Russian Federation and Ukraine. So, this is the first factor, this complex threat landscape, which also has associated characteristics inherent to cyberspace. The issue of decentralized management, anonymity, and the ease of carrying out actions with some degree of anonymity facilitate this complex threat landscape. Then we have another factor that relates to our society's inability to securely deal with the range of technologies or applications available today. Here, we clearly have a problem of a significant lack of digital literacy. This reflects both on the individual's ability to protect themselves as citizens and on organizations' ability to design, operate, and implement protective mechanisms. I mentioned three factors, but there is a third one that I can't remember. This is the general framework. My master's thesis is still relevant in this sense, focusing precisely on cybersecurity governance. What instruments does the state have to respond to this situation? It has the judicial and legal system, as a significant part of these instruments involves criminal offenses, and therefore, law enforcement agencies are responsible for identifying authors and bringing them to justice. Here we are talking about the deterrent aspect of criminal law, which does not work very well in cyberspace. It doesn't work because we clearly have a deficit of convictions in this domain, and therefore, it is essential that this axis of action becomes more

effective for overall state effectiveness. We have diplomacy, which is important concerning, for example, the application of sanctions to individuals or organizations involved in offensive actions in cyberspace. I recall, for instance, the European Cyber Diplomacy Toolbox, which has already applied some of these measures to hostile actors. And when diplomacy fails, we enter the realm of public international law, and we obviously have the axis of war, where offensive capabilities are unleashed by military forces. Then we have another significant axis. In my 2009 thesis, I called it "simple protection," but it may be easier to understand as "civil protection," which encompasses the concept of resilience. Individual resilience, which includes digital literacy, and organizational resilience, which involves resistance to attacks, the ability to recover, and incident response. This axis has a central actor, which is the National Cybersecurity Centre. But there are many other extremely important actors, such as academia, sector collaborators, and the industry itself, which plays a crucial role in organizational resilience, providing solutions that help protect and ensure business continuity. So, we have the continuity of business and activity as the main objective of this civil protection framework. We have the identification of authors and prosecution in criminal proceedings, diplomacy defending the state's interests, and in war, let's say, the muscular defence of the state's interests. These are the instruments that states have to combat these types of threats, which have two very particular characteristics: they are transnational, no country can solve this alone, and they also have an asymmetric nature. Obviously, in each of these axes, we have national and international structures. For example, in the civil protection axis, Portugal has a network of incident response teams, akin to a firefighters' league to deal with fires. I repeat, the focus is on business continuity. But we also have international networks. The National Cybersecurity Centre, for example, is part of a European network of incident response teams, which was established by the NIS Directive and is now being reinforced by the NIS 2 Directive. Similarly, the Judiciary Police, which is central to criminal investigations, has Europol as a European network for criminal prosecution and investigation. The diplomatic sphere has its network of contacts within the European Union's External Action Service, and the Cyber Defence Centre, now the Cyber Defence Command or something similar, obviously has NATO as a network of partners within the European Union. The public policies in this area are diverse, and Portugal is well positioned in all of them. In fact, the United Nations' Cybersecurity Public Policy Index raised Portugal from 42nd to 14th place between 2018 and 2020. Therefore, we are now expecting the next process to be launched, but from the perspective of public policies, we have some of the best international practices in this field. I'm not sure if I answered your question.

A.N.A. Yes, yes. The next question essentially is, what do you think is lacking, what still needs to be done both at the national level and potentially within NATO? What is needed to ensure better cybersecurity?

L.S. I still haven't understood. The way you're posing the question regarding NATO, I still haven't quite grasped how you're referring to cybersecurity within the scope of NATO.

A.N.A. Yes, well, I would say, perhaps, either cyber defence or cybersecurity in cyberspace. Because, as I discussed with the Admiral (António Gameiro Marques), cybersecurity is an aspect that is more closely related to the European Union, or where Portugal works more closely with the European Union to ensure its cybersecurity. Cyber defence, on the other hand, is more of a NATO concern, aimed at ensuring that cyber defence.

L.S. Exactly, because the military forces have a monopoly on the use of force. Now, the best phrase wouldn't be exactly like that, but the military has a monopoly on the use of force. However, these are two distinct things. We use the term "cyberspace security" precisely to avoid sensitivities regarding the subordination of these two concepts to each other. Therefore, with "cyberspace security," we are able to address both the defence aspect and the cybersecurity aspect. Cybersecurity itself, in my opinion, and it's a bit of the culture we have here at the National Cybersecurity Centre, we try to look at it in a holistic way. It's not just a matter of internal security, but also a market issue and a human rights issue, or "civil liberties." So, for us, cybersecurity has dimensions beyond internal security. Did you study Security Studies at the Copenhagen School? Mr. Barry Buzan was... in the 1980s, if I'm not mistaken, he coined the concept of broad security and the blurring of boundaries between traditional internal security and external security. It's something we can understand well today, but it was a bit innovative in the context of the Cold War. When we talk about national security, perhaps beyond defence and internal security, we have to consider issues such as environmental security, financial security, and human security. In fact, it was this concept that led the UN to introduce the concept of human security and enabled the UN to undertake peacekeeping missions in certain territories. If we integrate this concept within the scope of cybersecurity, we also consider these issues. That's why I mentioned regulators earlier in the context of the "simple protection" axis. We are no longer talking about national defence or national security. Portugal doesn't have a national security strategy. For example, the United States, England, and France do have one. Typically, under this national security strategy, there is a component of territorial defence, then we have an internal security strategy, and then we have other strategies. Here, the idea of "cyberspace security" is somewhat similar, integrating these various concepts. But I got lost, what was the question again?

A.N.A. The question was essentially, what is missing in the field of cybersecurity?

L.S. I was talking about this in relation to NATO. NATO is a defence alliance, and as a defence alliance, it should focus exclusively on the defence of its members as a whole. On the other hand, cybersecurity, as I mentioned, is more centred around resilience and civil protection, which is why I mentioned that in the European Union it is focused on the public market aspect. Do you see the idea I'm trying to convey? So, there are no offensive operations here, no active defence concepts. Instead, there is protection, tolerance for failures, and resilience to survive attacks, with a focus on business continuity. That's the perspective and the business of the National Cybersecurity Centre. In contrast, if there is an attack by a member state that could be considered an illegitimate use of force within the United Nations, it could trigger a legitimate defence and therefore a defensive action by a state or a group of states. So, that's the main difference between the two. Can you repeat the question again?

A.N.A. What is missing in the field of cybersecurity?

L.S. What is missing? A lot of things. We have some specific developments, but from a public policy standpoint, there is not much missing. From a public policy perspective, we have a set of commitments in the area of certification to fulfil. There are European legal instruments that are shaping this environment in new ways, such as the regulation of artificial intelligence and the regulation of digital services, on one hand, and a new proposal for regulation, what's it called in Portuguese? The Cyber Resilience Act, or CRA, it should be something like "cyber resilience regulation" or something similar, which focuses on regulating the development and sale of products and services in the field of cybersecurity, with a consumer protection logic. For example, it states that when someone buys a mobile phone, they expect to receive security updates for a certain number of years. Currently, there is no certainty regarding that. Furthermore, it regulates the software development according to a set of principles, such as Cyber Security by Design, so it's about regulating the creation and application of the market for cybersecurity products and services. Other things that need to be done: a strong focus on digital literacy. Digital literacy is essential to reduce the societal vulnerability I mentioned earlier. Regarding NATO, I think it's necessary to first examine whether the concept of deterrence also applies to cyberspace and cyberspace activities. Personally, I have many doubts. In other words, if an arms race in cyberspace is a differentiating element and contributes to peace, like other races, such as the arms race observed during the Cold War.

A.N.A. The idea I had about cybersecurity, reading the strategies of other countries...

L.S. They use the concept of cybersecurity... We use the concept of security of the cyberspace. But they use it because they have national security, national cybersecurity. Ours is just a small adaptation.

A.N.A. Yes, the idea I had, and I think Engineer [referring to L.S.] touched on it a bit, is that some countries have a more passive approach to cybersecurity, while others have a more active perspective. In other words, the more passive ones essentially don't attack, they don't do anything, they wait to be attacked and then respond or defend. Whereas the more active ones in their cybersecurity don't wait to be attacked. They either attack or keep attacking to prevent adversaries from targeting their nation. England and the United States are two cases that have this more offensive posture.

L.S. Yes, but that's already executed by the military. The strategy is cybersecurity, but it's equivalent to the security of the cyberspace, and that's a defence component.

A.N.A. Yes. Actually, I had the idea that, essentially, at least from what I understood in my reading, cybersecurity ensures the security of the cyberspace, including that aspect of pre-emptive attack to guarantee security. But in the case of an attack from another country, the cyber defence part comes into play. It deals with defending the cyberspace during the attack and potentially responding.

L.S. I don't think that has ever happened. Let's say... [moves away] I won't talk about it here, otherwise it won't be recorded. [Approaches] There's an interesting book by a journalist... What's his name? He talks exactly about the American posture regarding response to major attacks. And he gives the example of the Obama administration and the attack that was carried out against Sony. The attack on Sony was later attributed to the North Korean government, related to the movie that mocked...

A.N.A. Yes, that one.

L.S. Exactly. The reality is that the United States, despite it being an attack on American soil or with an impact on American soil, they did not retaliate precisely because it was a private company, and in my opinion, correctly so. Retaliating would actually lead other private companies to stop investing in their cybersecurity, as they would rely on the U.S. cyber defence to protect them. So, there are quite a few nuances regarding the question you just asked.

A.N.A. That was indeed the idea I had. For example, Germany is a country that has a more passive approach to cybersecurity, according to their strategy. France, I think, is also somewhat similar, although different, but they also have

a more... No, not France, Spain. Spain also has a similar posture, more passive. From what I've gathered, Portugal also has a more passive posture.

L.S. The cyberspace security strategy mentions the subject but doesn't elaborate. But if you look at the cyber defence strategy, it talks about developing offensive capabilities.

A.N.A. Yes, yes, indeed.

L.S. So, I would say that's where... I remember the British used a very interesting term, which was "cyberspace exploration." They didn't talk about attacking, but about exploring the cyberspace in terms of the interests of the United Kingdom.

A.N.A. I also have a vague idea of having read something like that in their strategy. Cyberspace Exploration.

L.S. But that... I don't know. I can't answer that. I know that many countries are developing capabilities. Most of them don't know what to do with it or how to do it. As a side effect, we have a thriving Dark Web selling vulnerabilities and creating a lively market for exploitable vulnerabilities, which does not contribute to a better cyberspace. A cyber weapon is a vulnerability known only to an agent. Those people who engage in hacking to find vulnerabilities, depending on the level of exposure that the exploitation of that vulnerability provides, can sell a vulnerability for $10 million on the Dark Web. What I... What should be done is to fix that vulnerability so that it cannot be used by malicious actors. In fact, a country that collects vulnerabilities in computer systems commonly used in its territory is doing a disservice to its community. It's called the "Ricochet Effect."

A.N.A. The next question was whether, as part of NATO, we are at the same level as other states like China and Russia, whether we are lagging behind or ahead.

L.S. From a capabilities standpoint?

A.N.A. Capabilities, essentially, yes.

L.S. This is extremely difficult to assess because what I think we can observe from what we know is that there are two countries that have been very successful in the defensive activities they develop... the exploration of cyberspace, using the generic term coined by the British. Russia started very

early and saw the potential of cyberspace for conducting espionage attacks, propaganda campaigns, and manipulation through cyberspace. They excel in the latter, being the first to realize the potential of cyberspace for such purposes. Then we have a set of countries that we know have offensive capabilities because they have been attributed a number of successful attacks. This includes China, Iran, North Korea... But it doesn't mean that Western powers don't have these same capabilities. I cannot compare them. I mean, I don't have the counterpart to know what kind of attacks countries like Israel, or England, or the United States carry out in their operations. I have no way to make a comparison.

A.N.A. The next question is essentially about the impact a cyber-attack can have today, whether it can cause significant damage or not.

L.S. That's a very easy answer, and I'll use it as an opportunity to provide some doctrine. An attack is only relevant when it has real-world impacts. And indeed, we had some examples last year, showing the disruptive potential, the real-world impact of a cyber-attack is enormous. The increasing dependence of essential services provided by both the state and private companies, which are vital to our life in society, relies heavily on information technologies. Information technologies have their vulnerabilities, and we also have another worrying element, which I mentioned earlier, which is the lack of expertise to implement good cybersecurity solutions, as well as the lack of digital literacy among the employees of these organizations, who can serve as an entry point for any threat actor. What do I mean by this? I mean that carrying out an attack with devastating effects does not require extraordinary capabilities on the part of the threat actor. It's the opposite. It's enough to find an employee of the target with low digital literacy and, let's say, manipulate them into providing credentials, as usual. So, carrying out a social engineering attack as an entry point, and once inside, using common techniques of simulation, lateral movement, privilege escalation, and infrastructure persistence to carry out a destructive attack. We saw this, for example, in the case of Vodafone last year. Even though Vodafone is a company with considerable resources and capabilities to respond to such a situation, they are not abundant. There are many companies providing vital services that lack capable human resources.

A.N.A. And they should have them.

L.S. Now, it won't happen overnight. But it will take a generation and a significant investment in literacy and specialized training. Because there are two dimensions here. One is that the general population needs digital literacy. In other words, knowing how to use devices in a secure manner. And the other is having specialized resources to protect organizations. These are two different things. In both cases, there are structural deficits, and these deficits are not a national problem, but a global one.

A.N.A. Does it take a generation to change that? Can't it be done sooner? Don't we remain vulnerable during that whole time?

L.S. We are gradually reducing vulnerability. There are two movements we are observing. One of them is that we are all investing in digital literacy and skills development. The National Cybersecurity Centre itself has created an academy to train six thousand specialists...

A.N.A. The C-Academy.

L.S. C-Academy, yes. There are other initiatives, public and private entities with the same objective. All of them are welcome because we have a huge deficit. This is an investment in retraining, precisely to bridge the generational gap, to reduce the time needed for the generation. It is not enough to rely solely on universities producing specialists; we need to invest in retraining the people we already have. Another aspect is digital literacy, which is commonly referred to as cyber hygiene, i.e., the fundamentals, the basics of cybersecurity to withstand these goat-like attacks, such as phishing or other social engineering techniques. Both are essential. Now, the other movement is the movement of regulation. The European Union, with the GDPR, initiated a trend of technology regulation like never before. It started a trend of regulating technology with the aim of protecting citizens from the negative impacts of that technology. The GDPR requires the completion of a Data Protection Impact Assessment (DPIA). Therefore, it mandates a prior assessment of the negative impacts that processing personal data may have on data circulation. The regulation on artificial intelligence has the same principle. It doesn't prohibit artificial intelligence, but for applications of AI mechanisms that may be considered high risk, it requires an impact assessment. If the impact is highly negative, the use of artificial intelligence is prohibited under the regulation. So, we are somehow working on empowering companies and organizations while also protecting ourselves from the negative impacts that technology can have. That's what we are observing in order to reduce the problem.

A.N.A. The next question is related to the legislative aspect, whether in the Portuguese case or in a more general case, which is: if the legislative part of countries can keep up with...

L.S. The evolution?

A.N.A. The evolution, yes.

L.S. No, it can't keep up, and we can't expect it to. It's a fact of life.

A.N.A. The Admiral (António Gameiro Marques) had mentioned that it would be best to have a more general law and the more specific aspects to be addressed through regulations, if I'm not mistaken. Do you agree with this approach?

L.S. By definition, legislation always lags behind. Legislation, in a way, informs how we live in society. And typically, it responds to specific problems, which makes sense. Therefore, we have to have that... There is always that act. The time between when the problem arises and when legislation responds. In criminal law, this happens, meaning when a problem of a certain offense arises and we realize that it's not covered by the criminal offenses in the code, an amendment is made to the criminal code to include that offense. And this is not specific to cyberspace; it applies to how legislation always responds to problems. So, we have to accept that. Now, what we can consider is whether we need to find more expedient methods to shorten the legislative cycle. In other words, I don't think we should legislate in a vacuum. Legislation is meant to address problems. However, we can try to shorten the process. What we observe today is that, especially if it's a European initiative in the technology field, initiatives have to be European. A single country cannot "stand up to" a tech giant. Perhaps the European Union as a whole can. Therefore, when it comes to regulating these applications, creating a regulation can take one to three years, and then we usually have an additional 24 months, 20 to 21 months for transposition into national legislation. It takes five years from the identification or the courage to address the problem until we have a legal framework to apply. I think we need to work on that aspect. In other words, reducing and shortening that process. Potentially, by focusing more on regulations, to avoid the transposition period into national legislation. Also, because, as I mentioned, when it comes to regulating technology as a norm, without market interests and tech giants involved... Therefore, a single country doesn't have the strength to do it, and it has to be done at the European level. But we should consider relying more on regulations and still try to shorten the legislative timeline.

A.N.A. Okay, we're essentially all done.

[END]

[START]

António Neves Almeida: Primeira pergunta que eu tinha era: qual é a sua visão sobre o atual estado de arte da cibersegurança num aspeto geral, num aspeto nacional e, eventualmente, no aspeto da NATO.

Lino Santos: Estado da arte da cibersegurança. Isso depende mais da definição de cibersegurança, não é propriamente consensual. Mas, devo dizer que acho que há três fatores que contribuem para uma elevada vulnerabilidade societal. Um primeiro fator diz respeito a um quadro de ameaças bastante sofisticado, que vai desde atores estatais, agentes de cibercrime, cibercrime organizado, até ativistas, portanto a convergência entre técnicas de hacking e ativismo político e ainda nesta categoria, sem motivação política, e depois alguns miúdos que, pelo desafio ou pela reputação entre pares, também desenvolvem atividades ilícitas no ciberespaço. Um quadro de ameaças complexo, onde é difícil fazer uma eficaz atribuição de responsabilidades, tanto como a diluição de fronteiras entre estes agentes que acabei de referir. Temos alguns exemplos concretos, desde ataques de falsa bandeira, até as milícias no ciberespaço com o grupo Killnet, do lado da Ucrânia existem grupos semelhantes que executam ataques de alguma forma com o plácito destes governos da Federação Russa e da Ucrânia. Portanto, este é o primeiro fator, este quadro complexo de ameaças que também têm associado a si algumas características que são inerentes ao ciberespaço. A questão de uma gestão descentralizada, a questão do anonimato, da facilidade em realizar ações com algum grau de anonimato, facilita este código de ameaças complexo. Depois temos um outro fator que diz respeito à incapacidade que temos como sociedade de lidar com, em segurança, com o conjunto das tecnologias, ou conjunto das aplicações, não das tecnologias, das aplicações, eu gostava de não colocar foco aqui na tecnologia, mas colocar na aplicação da tecnologia, o conjunto das aplicações que estão hoje disponibilizadas a esta sociedade, ou seja, aqui temos claramente um problema de literacia ou de falta de literacia digital muito grande. E isto reflete-se, quer na capacidade que nós temos individualmente de nos proteger como cidadão, quer na capacidade que as organizações têm de desenhar, operar, implementar mecanismos de proteção. Eu disse três fatores. Há um terceiro que não estou a lembrar. Este é o quadro genérico. A minha tese de mestrado continua atual nesse sentido e foi precisamente sobre governance da cibersegurança. Que instrumentos é que o Estado tem para reagir a este estado de coisas? Tem desde logo o sistema judicial e

judiciário, portanto grande parte destes instrumentos configuram ilícitos criminais e portanto os órgãos de investigação criminal são responsáveis por identificar autores e levá-los à justiça. E aqui estamos a falar da componente dissuasora do código penal, que não funciona muito bem no ciberespaço. Não funciona porque temos claramente um déficit de condenações neste domínio e, portanto, era essencial que este eixo de atuação fosse mais eficaz para o conjunto da eficácia do Estado. Temos a diplomacia e a diplomacia é importante no que diz respeito, por exemplo, à aplicação de sanções a indivíduos ou organizações que suportam ou conduzem ações ofensivas no ciberespaço. Estou-me a lembrar, por exemplo, da Toolbox Europeia de Ciberdiplomacia, que já aplicou algumas destas medidas a alguns agentes hostis, e quando a diplomacia falha, ou seja, subimos ao patamar do direito internacional público e temos obviamente o eixo da guerra, e aqui temos as capacidades ofensivas desencadeadas por forças militares. E depois temos um outro eixo bastante importante. Eu chamei na minha tese em 2009 "proteção simples", se calhar é mais fácil de perceber como "proteção civil", que tem toda a componente que hoje em dia designamos de resiliência. Resiliência individual, portanto, da literacia digital, resiliência das organizações, portanto, da resistência a ataques, a capacidade de recuperação, a resposta a incidentes. Eixo este que tem um ator central, que é o Centro Nacional de Cibersegurança. Mas tem um inúmero de outros atores extremamente importantes como a academia, como os colaboradores setoriais, a própria indústria tem um papel determinante neste capítulo da residência das organizações, tendo soluções que ajudem a proteger onde o objetivo é o business continuity. Portanto, temos a continuidade do negócio e da atividade que é o principal objetivo deste texto da proteção civil. Temos a identificação de autores e a condenação na prossecução criminal, temos na diplomacia a defesa dos interesses do Estado e na guerra, digamos, a defesa muscular dos interesses do Estado. Estes são os instrumentos que os Estados têm para combater este tipo de ameaças que têm duas características muito particulares que são transnacionais, nenhum país consegue resolver isto sozinho, e também têm uma natureza assimétrica. É óbvio que em cada um destes eixos temos estruturas nacionais e temos estruturas internacionais. Por exemplo, no eixo da proteção civil nós temos em Portugal uma rede de equipas de resposta a incidentes, fazendo uma analogia, uma espécie de liga de bombeiros para acudir a incêndios. Volto a repetir, o foco na continuidade de negócio. Mas também temos redes internacionais. O Centro Nacional de Cibersegurança, por exemplo, pertence a uma rede europeia de equipas de resposta a incidentes, que aliás foi criada pela Diretiva NIS e vem agora a ser reforçada com a Directiva NIS 2. Já a Polícia Judiciária, que é o elemento central na investigação criminal, tem a Europol como uma rede europeia para a prossecução criminal, para a

investigação criminal. Assim como a diplomacia tem a sua rede de contactos dentro do serviço de ação externa da União Europeia, e o centro de ciberdefesa, agora é o comando de ciberdefesa, ou alguma coisa desse género, tem obviamente a NATO como rede, aqui na União Europeia, como rede de parceiros. As políticas públicas desta área são das mais variadas e Portugal não está mal posicionado em nenhuma delas. Aliás, o índice de políticas públicas para a cibersegurança das Nações Unidas fez subir Portugal de 42º para o 14º lugar entre 2018 e 2020. Portanto, há de estar agora para ser lançado o próximo processo, mas do ponto de vista das políticas públicas temos das melhores práticas internacionais nesta área. Não sei se respondi à sua questão.

A.N.A. Sim, sim. Próxima pergunta é, essencialmente, o que é que acha que está em falta, o que é que falta fazer no aspeto nacional e no aspeto, eventualmente da NATO? O que é que falta para garantir uma melhor cibersegurança?

L.S. Eu ainda não percebi. A forma como está a colocar a questão relativamente à NATO. Eu ainda não percebi bem a forma como está a colocar a questão relativamente à NATO. Eu ainda não percebi bem o que é que quer dizer com a cibersegurança no âmbito da NATO.

A.N.A. Sim, pois, diria mais, se calhar, ou a ciberdefesa ou a segurança no ciberespaço. Porque, como falei com o Sr. Almirante, a cibersegurança é um aspeto que tem mais a ver com a União Europeia, ou que Portugal trabalha mais com a União Europeia para garantir a sua cibersegurança. E a ciberdefesa é um aspeto mais da NATO, para garantir essa ciberdefesa.

L.S. Exatamente, porque as forças militares têm o monopólio do uso da força. Agora, a melhor frase não seria desta maneira, mas os militares têm o monopólio do uso da força. Agora, são duas coisas distintas. Nós usamos a formulação "segurança do ciberespaço" exatamente para evitar sensibilidades no que diz respeito a uma subordinação destes dois conceitos entre si. E, portanto, conseguimos com "segurança do ciberespaço" falar numa componente de defesa e falar numa componente de cibersegurança. Cibersegurança em si, na minha opinião, e é um bocadinho essa cultura que nós temos aqui no Centro Nacional de Cibersegurança, tentamos olhar para ela de uma forma holística, ou seja, não é uma questão de segurança interna, mas é também uma questão de mercado e é também uma questão de direitos humanos, ou seja, "civil liberties" em português. Ou seja, para nós, cibersegurança não tem só a dimensão de segurança interna. Estudou o Security Studies da Escola de Copenhaga? O senhor Barry Buzan foi... na década salvo erro de 80, cunhou este conceito de segurança alargada e de diluição das fronteiras entre o tradicional segurança interna e segurança externa. E é uma coisa que hoje conseguimos perceber bem, mas no contexto de guerra fria foi um bocadinho inovador. Que é, quando falamos em segurança nacional, se calhar para além da defesa e para além da

segurança interna temos que olhar para questões como segurança ambiental, segurança financeira, segurança humana. Aliás, foi este conceito que levou a ONU vir surgir o conceito de segurança humana, e permitir à ONU fazer missões de paz em alguns territórios. Se integrarmos este conceito dentro do desígnio da cibersegurança também olhamos para esta questão, é por isso que falei de reguladores há pouco, no tal eixo de proteção de simples. Já não estamos a falar numa questão de defesa nacional ou de segurança nacional. Portugal não tem uma estratégia de segurança nacional. Por exemplo, os Estados Unidos têm, a Inglaterra tem, França tem. E normalmente, debaixo desta estratégia de segurança nacional, é que existe uma componente de defesa territorial, tipicamente territorial, depois temos uma estratégia de segurança interna e depois temos outras estratégias. Aqui a ideia da "segurança do ciberespaço" é um bocadinho o mesmo, a integrar destes diversos conceitos. Mas, perdi-me, qual era a pergunta?

A.N.A. A pergunta era, essencialmente, o que é que falta fazer no âmbito da cibersegurança?

L.S. Eu estava a falar disto por causa da NATO. A NATO é uma aliança de defesa. E sendo uma aliança de defesa deve se focar exclusivamente na questão da defesa do conjunto dos seus membros. A cibersegurança, por outro lado, trata, e daí ter dito que na União Europeia está centrada na questão do mercado público, trata mais no componente de resiliência e de proteção civil. Está a ver a ideia onde é que eu quero chegar. Portanto, não há aqui operações ofensivas, não há aqui defesa ativa, esse tipo de conceitos de defesa ativa. Existe sim a proteção disso e tolerância a falhas e sobrevivência a ataques de uma lógica de continuidade de negócio. É um bocadinho essa a perspetiva e um bocadinho esse o negócio do Centro Nacional de Cibersegurança. Por oposição a entender que se há um ataque por parte de um Estado membro que possa ser considerado o uso da força ilegítima no âmbito das Nações Unidas, possa disputar uma legítima defesa e portanto uma ação defensiva por parte de um Estado ou do conjunto dos Estados. Portanto, é um bocadinho esta a grande diferença entre as duas coisas. Pode repetir outra vez a pergunta?

A.N.A. O que é que falta fazer no âmbito da cibersegurança?

L.S. O que é que falta fazer? Muita coisa. Temos alguns desenvolvimentos pontuais, mas do ponto de vista de políticas públicas não falta muito. Do ponto de vista de políticas públicas temos aqui um conjunto de apostas na área da certificação a fazer. Há instrumentos legais europeus que vêm moldar um bocadinho de novo este ambiente, como por exemplo as questões relativas à regulação da inteligência artificial, as questões relativas à regulação dos serviços digitais, por um lado, e por outro, uma nova proposta de regulamento, como é que se chama em português? O Cyber Resilience Act, ou CRA, há de ser qualquer coisa como "regulamento de ciberresiliência", ou alguma coisa do género, que tem uma aposta na... que vem regular o desenvolvimento e a venda de produtos e serviços na área da cibersegurança, aqui um bocadinho uma lógica

da defesa do consumidor. Ou seja, vem por exemplo dizer que quem compra um telemóvel está à espera que isto tenha updates de segurança durante X anos. Hoje em dia não existe essa certeza. Mais, que o software que foi aqui desenvolvido segundo um conjunto de princípios, Cyber Security by Design, portanto, a regulação da criação e aplicação do mercado de produtos e serviços. Mais coisas que é preciso fazer: e é preciso apostar muito na literacia digital. A literacia digital é fundamental para diminuir aquela vulnerabilidade sociatal que eu referi acima. Relativamente à NATO, eu acho que é preciso fazer um exercício antes de mais, que é perceber se o conceito de dissuasão também se aplica ao ciberespaço e à atuação do ciberespaço. Pessoalmente tenho muitas dúvidas. Ou seja, se uma corrida às ciberarmas é um elemento diferenciador e contribui para a paz, como outras corridas, como uma corrida às armas que observamos no tempo da Guerra Fria.

A.N.A. A ideia que eu tinha de cibersegurança, lendo outras estratégias de cibersegurança de outros países...

L.S. Eles usam o conceito de cibersegurança... Nós é que usamos de segurança do ciberespaço. Mas eles usam, lá está, porque eles têm segurança nacional, cibersegurança nacional. O nosso é uma pequena adaptaçãozinha.

A.N.A. Pois é, a ideia que eu tinha, que acho que o Sr. Engenheiro até tocou um bocado nisso, é que alguns países têm uma postura mais passiva na sua cibersegurança e outros têm uma perspetiva mais ativa na sua cibersegurança. Ou seja, os mais passivos essencialmente não atacam, não fazem nada, ficam ali à espera de serem atacados e depois respondem ou defendem. Enquanto os mais ativos na sua cibersegurança não ficam à espera de serem atacados. Eles atacam ou vão atacando para não dar abertura aos adversários para atacarem a nação em causa. A Inglaterra e os Estados Unidos, são dois casos que têm essa postura mais ofensiva.

L.S. Sim, agora isso já seja executado pelos militares. Mas a estratégia é de cibersegurança, mas é o equivalente da segurança do ciberespaço e isso é uma componente de defesa.

A.N.A. Sim. Por acaso, tinha a ideia que, essencialmente, pelo menos também do que eu percebi na minha leitura, é que a cibersegurança garantia a segurança do ciberespaço, incluindo esse aspeto de ataque, "preemptive attack", para garantir a segurança, mas no caso de haver um ataque de outro país, entrava a parte da ciberdefesa. Pois tratava da defesa do ciberespaço durante esse ataque e eventualmente a resposta.

L.S. Eu acho que nunca aconteceu. Digamos, [afasta-se] eu não falo aqui porque senão não me grava. [Aproxima-se] Há um livro muito giro de um jornalista... Como é que ele se chama? Que fala exatamente da postura norte

americana relativamente à resposta a ataques, a grandes ataques. E dá o exemplo na administração Obama do ataque que foi realizado contra a Sony. O ataque realizado contra a Sony foi depois atribuído ao governo norte coreano, isto a ver com o filme a gozar com...

A.N.A. Sim, o tal.

L.S. Exatamente. A realidade é que os Estados Unidos, apesar de ter sido um ataque realizado contra o solo norte americano, ou com impacto em solo norte americano, eles não retaliaram exatamente por se tratar de uma empresa privada e, na minha opinião, corretamente, porque isso iria, na realidade, levar a que outras empresas privadas deixassem de investir na sua cibersegurança, porque a ciberdefesa norte americana estaria lá para os segurar. Portanto, há aqui bastantes nuances relativamente a essa questão que acabou de colocar.

A.N.A. Era, de facto, a ideia que eu tinha. Por exemplo, a Alemanha é um país que tem uma postura mais passiva na sua cibersegurança, segundo a estratégia deles. A França também acho que é mais ou menos a mesma coisa, embora diferente, mas também tem uma postura mais... Não, a França não, a Espanha. A Espanha também tem uma postura semelhante, é mais passiva. Portugal, do que eu já percebi, também tem uma postura mais passiva.

L.S. A estratégia de segurança do ciberespaço fala no assunto, não desenvolve. Mas se for ver a estratégia de ciberdefesa, fala em desenvolvimento de capacidades ofensivas.

A.N.A. Sim, sim, sim.

L.S. Portanto, eu diria que aí está ao nível... Eu lembro que os ingleses utilizavam um termo bastante interessante, que era a "exploração do ciberespaço". Não falavam em atacar, mas falavam em explorar o ciberespaço, a nível dos interesses do Reino Unido.

A.N.A. Também tenho uma vaga ideia de ter lido qualquer coisa do género na estratégia deles. Cyberspace Exploration.

L.S. Mas isso... Não sei. Não sei responder. Sei que há uma data de países que estão a desenvolver capacidades. A grande parte deles não sabe o que é que há de fazer com aquilo, nem como fazer aquilo. Isso cria como efeito secundário nós termos uma Dark Web a vender vulnerabilidades, e a criar um mercado de vulnerabilidades para ser exploradas bastante vivo e isso não contribui para um melhor ciberespaço. Ciberarma é uma vulnerabilidade que é só do conhecimento de um agente. Aquelas pessoas que se dedicam a fazer hacking

para encontrar vulnerabilidades encontram uma vulnerabilidade, dependendo do grau de exposição que a exploração daquela vulnerabilidade dá, uma vulnerabilidade pode custar $10 milhões à venda na Dark Web. O que eu... Um tratamento que devia ser dado àquilo era corrigir aquela vulnerabilidade para que não fosse usada por agentes maliciosos. Aliás, um país que coleciona vulnerabilidades em sistemas informáticos que são comumente usados no seu território está a fazer um péssimo serviço à sua comunidade. Chamado "Efeito Ricochete".

A.N.A. A pergunta a seguir era se enquanto NATO, se nós, comparando com outros Estados, como a China, a Rússia, se nós estamos ao mesmo nível, se estamos para trás, se estamos mais à frente?

L.S. Do ponto de vista de capacidades?

A.N.A. Capacidades, essencialmente, sim.

L.S. Isto é extremamente difícil de avaliar. Porque, o que eu acho que nós podemos observar daquilo que conhecemos é que há dois países que têm muito sucesso com as atividades defensivas que desenvolvem... A exploração do ciberespaço, usando o termo genérico dos ingleses. A Rússia começou muito cedo e viu o potencial do ciberespaço quer para a realização de ataques com vista à espionagem, quer a realização de campanhas de propaganda e de manipulação através do ciberespaço. Estes que são magos nesta última, e foram os primeiros a perceber o potencial do ciberespaço para isto. E depois temos um conjunto de países que a gente sabe que têm capacidades ofensivas porque é-lhes atribuído um conjunto de ataques bem-sucedidos. E aqui incluem-se a China, o Irão, o Coreia do Norte... O que não quer dizer que potências ocidentais não tenham essas mesmas capacidades. Eu não os consigo comparar. Ou seja, não tenho um efeito do outro lado para saber que tipo de ataques é que países como Israel, ou como Inglaterra, ou como os Estados Unidos executam na sua ação. Eu não tenho uma forma de poder comparar.

A.N.A. A próxima pergunta é, essencialmente, que impacto pode ter um ciberataque hoje, ou seja, pode ter impactos muito grandes em termos de danos ou...?

L.S. Isso é uma resposta muito fácil, aproveito para ir fazendo doutrina. Um ataque só é relevante quando tem impactos no mundo real. E, efetivamente, já tivemos alguns exemplos no ano passado e o potencial disruptivo, ou seja, de impacto no mundo real de um ataque realizado através de ciberespaço é enorme. A dependência, a cada vez maior dependência, que é aquilo que são serviços essenciais prestados quer pelo Estado, quer por empresas privadas, e que são essenciais para, são vitais para a nossa vida em sociedade, são muito dependentes de tecnologias de informação. Tecnologias de informação que têm

as suas vulnerabilidades e onde temos também, e onde temos um outro elemento preocupante, que foi aquilo que eu referi no início, que é a falta de massa cinzenta para implementar boas soluções de cibersegurança, e ainda a falta de literacia digital dos funcionários destas organizações que podem servir como porta de entrada de qualquer agente de ameaça. O que é que eu quero dizer com isto? Quero dizer que realizar um ataque com efeitos devastadores não necessita de capacidades extraordinárias por parte do agente de ameaça. É o contrário. Basta encontrar um funcionário do alvo com baixa literacia digital e, digamos, manipulá-lo a fornecer as credenciais, a costume, portanto, a realização de um ataque de engenharia social como porta de entrada e depois de estar lá dentro usar técnicas comuns de simulação, de movimentos laterais, de escalagem de privilégios, de persistência na infraestrutura até realizar um ataque destrutivo. Vimos isso, por exemplo, com o caso da Vodafone no ano passado. Sendo que a Vodafone até é uma empresa que tem muitos recursos e recursos capazes para reagir a uma situação destas. Mas não são muitas. E há muitas empresas que prestam serviços vitais que não têm recursos humanos capazes.

A.N.A. E deviam ter.

L.S. Agora, não vai de dia para a noite. Mas será preciso uma geração e uma aposta muito grande na literacia e na formação especializada. Porque há aqui duas dimensões, uma delas é a população em geral necessita de literacia digital. Ou seja, saber usar os equipamentos de uma forma segura. E outra é ter recursos especializados para proteger a organização. São duas coisas diferentes. Em ambas existem déficits estruturais, e défices estruturais, não é um problema nacional. É um problema global.

A.N.A. E é preciso uma geração para mudar isso? Não pode ser feito antes? Não ficamos vulneráveis durante esse tempo todo?

L.S. Vamos reduzindo a vulnerabilidade. Há aqui dois movimentos que estamos a observar. Um deles é que estamos todos a apostar nesta literacia digital e no desenvolvimento de competências. O próprio Centro Nacional de Cibersegurança criou uma academia para formar seis mil especialistas...

A.N.A. A C-Academy.

L.S. C-Academy, sim. Existem outras iniciativas, entidades públicas e privadas com o mesmo objetivo. Todas elas são bem-vindas, porque temos um défice brutal. Isto é uma aposta na requalificação, exatamente para diminuir essa distância da geração, esse tempo da geração. Não chega ao débito que as universidades têm especialistas, precisamos apostar na requalificação das pessoas que temos. Outra questão é a literacia digital, ou seja, aquilo que normalmente se designa de ciberhigiene, ou seja, os fundamentos, os básicos da cibersegurança para resistir a estes ataques de lana-caprina, como por exemplo,

o phishing ou outras técnicas da engenharia social. As duas são essenciais. Agora, o outro movimento é o movimento de regulação. A União Europeia, com o RGPD, inaugurou uma tendência de regulação da tecnologia como nunca tinha sido vista. Ou seja, inaugurou uma tendência de regulação da tecnologia tendo em conta a proteção dos cidadãos relativamente aos impactos negativos dessa tecnologia. O RGPD obriga a realização de um Data Protection Impact Assessment, o DPIA. Portanto, obriga a uma avaliação prévia de quais são os impactos negativos que aquele processamento de dados pessoais pode trazer no circular dos dados. O regulamento da inteligência artificial tem a mesma coisa. Não proíbe a inteligência artificial, mas para aplicações de mecanismos de inteligência artificial que possam ser considerados de alto risco obrigam a uma avaliação de impacto. E se o impacto for muito negativo, essa utilização da inteligência artificial está proibida no regulamento. Ou seja, estamos de alguma forma a trabalhar a capacitação das empresas e das organizações, mas ao mesmo tempo a protegermo-nos dos impactos negativos que a tecnologia possa ter. É isso que estamos a observar para tentar reduzir o problema.

A.N.A. A próxima pergunta tem haver com o aspeto legislativo, pode ser no caso português, pode ser num caso mais geral, que é: se a parte legislativa dos países conseguem acompanhar...

L.S. A evolução?

A.N.A. A evolução sim.

L.S. Não. Não consegue nem podemos estar à espera que consiga. É um facto da vida.

A.N.A. O senhor Almirante (António Gameiro Marques) tinha dito que o melhor era haver uma lei mais geral e as partes mais especificas serem feitas através de regulamentos, se não me engano. Concorda com essa abordagem?

L.S. Por definição, a legislação vem sempre atrás. A legislação, de alguma forma, vem a informar a forma como nós vivemos em sociedade. E por norma, ela vem responder a problemas específicos, faz sentido. E, portanto, nós temos que ter esse... Existe sempre esse ato. O tempo entre o problema surge e a legislação vem responder. No código penal isso acontece, quer dizer, quando surge um problema de algum tipo de penal que verificamos que não está coberto pelos tipos penais do código, faz-se uma alteração ao código penal, introduzindo esse tipo de penal e isso não tem a ver com o ciberespaço, tem a ver com a forma como... A legislação vem sempre responder a problemas. E portanto, temos que assumir isso. Agora, o que podemos é equacionar se não temos que encontrar métodos mais expeditos de encurtar o ciclo legislativo. Ou seja, a priori não acho que se deve a legislar no vazio. A legislação é para responder a problemas. Podemos é tentar encurtar. O que nós observamos hoje é que principalmente se

for uma iniciativa europeia, nesta área da tecnologia... As iniciativas têm que ser europeias. Um país sozinho não pode, não consegue "fazer frente", a um gigante tecnológico. Se calhar o conjunto da União, consegue. Portanto, quando se trata de regular estas aplicações, fazer um regulamento pode demorar um ano, um ano e meio a três anos e depois temos mais, normalmente, mais 24 meses, 20, 21 meses para a transposição para a Legislação Nacional. Faz cinco anos, desde que se identifica ou se tem a coragem de adressar o problema, até nos países temos, se for uma diretiva, em transposição só se aplica se for uma diretiva, até termos um corpo legal para aplicar, eu acho que temos de trabalhar aí. Ou seja, em reduzir, em encurtar esse ato. Eventualmente, apostando mais em regulamentos, para não ter o período de transposição para a legislação nacional. Até porque, volto a dizer quando se trata de regular tecnologia como norma, mas sem interesses do mercado e das gigantes tecnológicas... Portanto, um país sozinho não tem força para o fazer, e terá que ser feito a nível europeu, mas apostar mais em regulamentos e tentar mesmo assim cortar o prazo de legislação.

A.N.A. Ok, está essencialmente tudo feito.

[END]

PAGE LEFT INTENTIONALLY BLANK