Centro Universitário de Brasília - UniCEUB

Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito / Curso de Bacharelado em Relações Internacionais

GABRIELA ROBL ZITTA

TO WHAT EXTENT HAVE THE FRAMEWORKS ADOPTED BY THE EUROPEAN UNION PROVED EFFECTIVE IN CYBERSPACE?

BRASÍLIA
2024

GABRIELA ROBL ZITTA

TO WHAT EXTENT HAVE THE FRAMEWORKS ADOPTED BY THE EUROPEAN UNION PROVED EFFECTIVE IN CYBERSPACE?

Scientific article presented as a partial requirement for obtaining the title of Bachelor of Law/Bachelor of International Relations from the Faculty of Legal and Social Sciences - FAJS of the Centro Universitário de Brasília (UniCEUB).

Advisor: Oscar Medeiros Filho

BRASÍLIA
2024

GABRIELA ROBL ZITTA

TO WHAT EXTENT HAVE THE FRAMEWORKS ADOPTED BY THE EUROPEAN UNION PROVED EFFECTIVE IN CYBERSPACE?

Scientific article presented as a partial requirement for obtaining the title of Bachelor of Law/Bachelor of International Relations from the Faculty of Legal and Social Sciences - FAJS of the Centro Universitário de Brasília (UniCEUB).

Advisor: Oscar Medeiros Filho

BRASÍLIA, OCTOBER 29th 2024

EVALUATION BOARD

____

Advisor Teacher

____

Evaluator Teacher

ACKNOWLEDGMENTS

As a wise man once said, I´d like to thank me for believing in me, for doing the hard work, and for never quitting, therefore I am grateful for this journey and the growth it came with.

TO WHAT EXTENT HAVE THE FRAMEWORKS ADOPTED BY THE EUROPEAN UNION PROVED EFFECTIVE IN CYBERSPACE?

GABRIELA ROBL ZITTA

ABSTRACT

Cyberspace is an intangible and decentralized domain that transcends the normal physical boundaries and allows for better connectivity, however, it presents significant risks. The rapid technological advances redefined the international relations and the common national security strategies, given the reliance on digital infrastructures. This thesis aims on exploring the intersection of cyberspace governance and international cooperation frameworks, particularly through the lens of neoliberal institutionalism. While examining the role of international agents such as the EU, it´s regulatory frameworks and NATO, it is noted how global governance has adapted to mitigate cyber threats. Key frameworks like the General Data Protection Regulation (GDPR) and the NIS Directive have been essential in promoting collective measures for cyberspace across Member States. Through case studies like the SolarWinds, NotPetya and WannaCry attacks, this article evaluates the effectiveness of said frameworks in ensuring cyber resilience, addressing cross-border challenges while enhancing a more productive cooperation between state and non-state actors.

Key words: cyberspace; frameworks; transnational cooperation; collective security and cyber governance.

EM QUE MEDIDA OS QUADROS ADOTADOS PELA UNIÃO EUROPEIA SE PROVARAM EFICIENTES NO CIBERESPAÇO?

GABRIELA ROBL ZITTA

RESUMO

O ciberespaço é um domínio intangível e descentralizado que transcende as fronteiras físicas normais e permite uma melhor conectividade, mas apresenta riscos significativos. Os rápidos avanços tecnológicos redefiniram as relações internacionais e as estratégias comuns de segurança nacional, dada a dependência de infraestruturas digitais. Esta tese visa explorar a intersecção entre a governação do ciberespaço e os quadros de cooperação internacional, particularmente através das lentes do institucionalismo neoliberal. Ao examinar o papel dos agentes internacionais como a UE, os seus quadros regulamentares e a NATO, nota-se como a governação global se adaptou para mitigar as ameaças cibernéticas. Quadros fundamentais como o Regulamento Geral sobre a Proteção de Dados (RGPD) e a Diretiva SRI têm sido essenciais na promoção de medidas coletivas para o ciberespaço nos Estados-Membros. Através de estudos de caso como os ataques SolarWinds, NotPetya e WannaCry, este artigo avalia a eficácia dessas estruturas para garantir a resiliência cibernética, abordando desafios transfronteiriços e, ao mesmo tempo, melhorando uma cooperação mais produtiva entre intervenientes estatais e não estatais.

Palavras-chave : ciberespaço; regulações; cooperação transnacional; segurança colectiva e governação cibernética.

INTRODUCTION

The fast growth of cyberspace revolutionized the landscape of international relations and global governance. Unlike the normal physical domains, the cyberspace- referred to as C.S. in this thesis- is a vast intangible interconnected digital environment. This domain ecompasses the flow of data, networks, communication, software systems and the internet itself. Considering the decentralized nature and the speedy pace of digital interactions, this transcends boundaries and sets a unique risk and vulnerabilities for countries, making C.S. not only a facilitator of global connectivity but also a highly contested space with far-reaching implications for international security and sovereignty.

From a neoliberal institutionalist perspective, we can understand the increased importance of international institutions and cooperative frameworks in managing cyberspace. The Impacts of C.S. in international relations shall not be overstated, since it fundamentally alters how states interact, how diplomacy and security works nowadays and the dissemination of information. The evolution of cyber threats underscores the need for comprehensive security strategies, while increasing the resilience on digital infrastructures.

Therefore, the effectiveness of the frameworks adopted by the EU in promoting a better coordinated and secure international response is evaluated and highly important. Seeking to provide a comprehensive understanding of the role that international institutions and frameworks have in governing cyberspace, as well as the discourse of how states can navigate the complexities of cyberspace and establish an overreaching legal and regulatory mechanism for cyber threats.

1 INTRODUCTION TO CYBERSPACE AND NEOLIBERAL INSTITUTIONALISM

1.1 Definition and characteristics of cyberspace

The intangibility of cyberspace allows it for such a hard determination of its definition, the interconnected digital environment created within the global network of information and communication technologies (ICTs) is vast and unlike any other traditional physical domain. Not necessarily in the traditional scopes such as air, land, sea and space, the cyberSpace (C.S), referred to in this present article as C.S, can be noted as a virtual construct that englobes the interconnectivity of data, information, softwares and internet.

From the perspective of neoliberal institutionalism in bestowal with Adwaith (2022), international institutions and cooperation frameworks present a vital role in addressing these risks and vulnerabilities. Institutions like the International Telecommunication Union (ITU) and initiatives like the Tallinn Manual 2.0 highlight the role that international governance can play in promoting shared rules and its aims to mitigate threats, with the establishment of global norms for cyberspace, States can collaborate on shared challenges that transcend borders, enhancing collective security and stability in this domain.

Transcending geographical boundaries, this virtual space that allows for such rapid digital interactions to occur, is seen as a global domain with frequent flow of data in real time, with a decentralized architecture, leaving no single entity to take control of said space, showcasing its risks and vulnerabilities.

1.2 Importance of C.S. in International Relations

The cyberspace has changed how States interact, impacting the International Relations in many dimensions, such as the change in formality in diplomacy and statal interactions, With such a rapid flow of communication and information spread, the C.S. allows for state and nonstate actors to engage diplomatically through digital platforms, outreaching and negotiating with ease. "Cybersecurity is national security. The frontlines of modern defense are no longer just on land, sea, and air, but also in the digital domain" (Nye, 2011, p. 132), with the aforementioned quote, we can establish the ongoing importance and emphasis that cyberspace has in this critical area for national and international security currently.

The national security level needs to be cared for in a deeper level, since governmental operations rely every day more on C.S., they are presented daily with threats such as espionage, hacking, phishing, that can destabilize the government itself, its economy and its relations with the international community.

Consequently, the intangibility in cyberspace complicates its politics and security strategies, as well as its definition. Unlike the physical aspects of a domain, where jurisdiction, borders and frontiers are well established, the cyberspace transcends those geographical and political spaces, meaning that if an attack were to be launched from anywhere in the world, its answers would be restricted according to the legal impositions and national sovereignty. However, neoliberal institutionalism argues that through multilateral cooperation and shared governance, states can work together within existing international frameworks to overcome these jurisdictional challenges, where institutions would be able to serve as platforms for coordination, ensuring that responses to cyber threats are harmonized and that legal gaps across borders are addressed.

1.3 The transnational and decentralized nature of C.S.

The separation of cyberspace is multifaceted, including from the physical sides of the infrastructure like servers, data centers, routers and many others, to the digital side like emails, websites, data transfer etc. becoming an important piece of our everyday life, in accordance with Moynihan (2021), cyberspace controls commerce, communications, from the simplest information to a national security detail. Additionally, the non tangible side of C.S. allows for threats and vulnerabilities to grow and spread faster, showcasing that the legal frameworks and regulatory structures can become obsolete if not developed with flexible and in-depth considerations, allowing for fast adjustments in the cybernetic scenario. In line with neoliberal institutionalist thinking, updating and reinforcing international legal frameworks is crucial, since the constant evolution of technology demands that institutions adapt swiftly, promoting regulations and protocols that facilitate cooperation and trust between states, as seen in efforts like the Budapest Convention on Cybercrime (2001), which harmonizes legal responses to cyber threats across different jurisdictions.

Attributes of cyberspace such as 1- its capability to obscure the identity and location of actors due to the use of proxies, 2- the ease on communication, speed, volume and reach it can have, even in remote places and poor regions and 3- the low-cost high value it has, considering most devices offer the basic requirements for data and connection and it's become easier and cheaper with time. Those attributes allow for growth opportunities, for civilians to interact in a more inclusive society, a new way to deliver goods and services, but also new means to be exploited by selected bad-intentioned actors. Given these vulnerabilities, and using our theoretical lense, we can see how it emphasizes the importance of collective action. International institutions can facilitate cooperation in addressing issues like anonymity and cybercrime, promoting transparency, and reducing the potential for exploitation by malicious actors, considerably through frameworks like the European Union's General Data Protection Regulation (GDPR), states can collaborate to secure data protection and privacy across borders.

Transcending national and conventional borders, the cyberspace undermines the traditional concept of state sovereignty, given its fast spread, communication and data flow across nations, its lack of centralized governance or control can certainly hinder the legal accountability and further issues. With ease on anonymity and obfuscation, malicious actions won't always be traceable, and this leads to the accountability on international law, that fails, as it was assigned to be used in a physical domain, as elucidated by Farrell on the challenges in traditional frameworks, "Jurisdiction in cyberspace is a complex and often contentious issue, as actions taken in one country can have effects across multiple borders, creating a tangle of conflicting laws and regulations" (Farrell, 2019, p. 53).

2 ACTORS IN CYBERSPACE

2.1 Diversity of actors

Cyberspace is notoriously used for intelligence gathering, military operations, espionage, hacking and many others, but to differentiate the actors and intentions to properly address it, is a major need. Government and State sponsored entities usually rely on significant resources and capabilities that allow for their actions to be so impactful on an international basis, as where non-state actors such as NGOs and individuals tend to bring more innovation and tend to shape the policies and governance frameworks inside C.S.. Criminals on the other hand, exploit the vulnerabilities and disrupt systems in order to receive compensation with the rise of said illegal actions, "As cybercriminals exploit the concealment offered by digital platforms, the range of their activities—from financial scams to critical infrastructure sabotage—has expanded significantly, posing severe risks on a global scale." (McGuire, 2021, p.74)

Hybrid actors are the ones that operate at the intersection of state and non-state entities, such as people that are privately funded but align with or are supported by state interests can engage in cyber operations with geopolitical implications, the case to be discussed further in this article, the SolarWinds attack in 2019 could be identified as involving hybrid actors giving the believed state sponsorship from Russian Foreign Intelligence Service (SVR) to the group APT29 (a.k.a. Cozy Bear), its objectives and meticulous execution, that following with Rid, "The SolarWinds hack is a prime example of how state-sponsored actors use private sector infrastructure to advance geopolitical goals, blurring the lines between national and private interests." (Rid, 2018, p. 493)

2.2 The complexity of identifying the origin of attacks

Cyber attacks are a deliberate, malicious action that seeks to compromise the confidentiality, integrity, or availability of computer systems, networks, or digital information, and have become increasingly constant in our society due to the technological advances we are witnessing, and the lack of legislation regarding the protection of cyberspace, which cannot be easily delimited by a border, unlike countries, since it encompasses a parallel reality where access to regions that in theory would be "sealed off" becomes easier and faster, as delimited by “We face not an easily discernible, relatively quantifiable threat but a multiplicity of hidden, ever-changing threats” (Bolton, 2021, p. 2).

Characterized as attempts to access a system without authorization, disable it or even steal it, violating its security, cyber attacks use a variety of methods, from malware, phishing, ransomware to man-in-the-middle attacks, as Ajayi (2016) discusses, bearing in mind that these attacks aim to damage a network system, gaining control or access to documents on a personal or commercial network

In accordance with Freedman (2023), hacker attacks have been on the rise in recent years, with growth from 15% per year until 2019, to 38% in 2022, highlighting the intensification of cyber attacks. Studies show that China, Russia and other nations have begun to offer some kind of shelter to these criminals as well as funding for hackers in various countries, causing a greater "incentive" in breaches of systems ranging from government agencies to small businesses, reaching users of networks such as X (formerly Twitter) and civilians.

The more a public service or infrastructure is digitized, the bigger the area for attacks becomes, providing more opportunities to infiltrate in the system and access sensitive information. Since espionage activities rely on data harvesting and collecting massive amounts of information, financial records, personal information, trade secrets, etc, those datas can be used in many malicious ways such as identity theft and financial fraud, that impact directly on e-commerce and other platforms.

2.3 The difficulty in attributing these attacks

Considerably, with the rise of sophisticated methods used by hackers to erase their digital footprints, gathering enough evidence for attribution can be quite complicated. Swerving the investigators with intentional misleading methods, using spoofed IP addresses, compromised servers and many techniques that are created on a day basis as the technology evolves, they get to successfully maneuver through investigations and depending on the geopolitical considerations of the area, as well as the technical challenges that might be presented they can successfully escape the attribution of an attack, as per mentioned by Rid (2015), attributing cyber attacks can be fraught with geopolitical implications, where international relations and political considerations may impact the process and outcomes of attribution.

3 DIFFICULTIES OF SECURITIZATION

3.1 Challenges in securitizing C.S. compared to physical space

Keeping in mind its ‘borderless’ characteristics, its global reach and constant change, cyberspace becomes a bigger securitization problem. With the lack of attribution constantly noted in C.S., as well as the rapid evolution of threats, the challenges to secure this area are bigger than ever. Further complications in the C.S. can be pinned on the anonymity given by it, allowing attackers to hide their identities and maneuver between locations, devices, and slipping through the cracks. Moreover, the decentralization of said space imposes bigger challenges in regulamentation and safety, in as much as not having a central entity controlling its core, laws and its applications, different jurisdictions can and do have different legislations that enable conflicts and makes accountability more difficult, where said decentralization enables for international cooperation to be even more crucial. Institutions like the United Nations and NATO's Cyber Defense Centre of Excellence, as seen with the Tallinn Manual 2.0, aim to help the States align its interests and efforts in order to establish norms and gain trust within C.S. governance, aiming to address the clash between different jurisdictions.

3.2The lack of international consensus on C.S. standards

The International Telecommunication Union (ITU) is the organization responsible for advising on cyber security, under the auspices of the UN, where protocols are suggested for members and participants to follow. However, according to Roaten (2022), it is not possible to demand that states come to a common understanding and define among all countries and their different legislatures, legal and judicial systems, the application of the same laws that address the virtual area and the invasion of online property, as this would initiate a political clash, due to the varying priorities and frameworks of different nations. Considerably, States disagree on cybersecurity regulations, resulting in loopholes in which hackers can handle information in illegal ways without being punished. If observed through a neoliberal institutionalist point of view, international institutions would mediate and allow for better dialogues between States, therefore reducing the chances of conflicts and building cooperation and mutual trust, setting aside their divergent approach to C.S.

If we consider that each State is able to choose its regulations and laws to be followed in the field of cybersecurity, as long as they fall within a protocol stipulated by the federation, this means that a State could take advantage, even unintentionally, of another State or even its citizens, thus leaving a kind of gap between the protection of a country and putting it at risk of international interventions, as mentioned by Brzostek (2022).

With the increased usage of the internet comes a problem with the intensified competition of it and its space and use, therefore in order to maintain proper security for the data, systems and artificial intelligence that is being used, rules need to be placed in international cyberspace. International rules and norms for cyberspace are critical for managing this competition and ensuring that the global digital environment remains secure and cooperative. Institutions like the UN and NATO can play key roles in fostering these rules and ensuring compliance across borders.

Hu (2019) affirms that the prices of wars now don't even compare to prior decades, since it's not necessary to buy guns and ammunition in order to attack, you can do so with just a click of a button, which gives terrorists and criminals a bigger area to work with and more possibilities and a bigger frequency for them to do so.

After analyzing the two main downsides of a cyber attack, being the cost of a data breach and losing the public's trust, you can identify the efforts made by many organizations to keep cybercriminals away, however, the fast growth of technology and weapons used by hackers to gain access illegally to a server as well as their enormous knowledge on said matter, it is nearly impossible to stop an intrusion, but there are things that can be done in order to lower the losses and access an individual can have, following the publication by Barker (2019).

3.3 Exemplifying the C.S. and attacks suffered

At this juncture, the attack suffered by SolarWinds is an excellent example of how cybersecurity can be used to undermine international security across the board. In 2019, the software company - responsible for providing network management and monitoring services to various US government agencies and private companies - was exposed to a sophisticated cyber attack, in which hackers successfully compromised its Orion software, used by millions of customers around the world, with the hackers allegedly being affiliated with Russia.

Despite this, the global impact of the attack is clear, with several US government agencies, including the Treasury and Energy Departments, the Pentagon and the White House, as well as private companies in other countries being affected. The hackers accessed sensitive information such as emails, documents and user credentials, raising concerns about national security, privacy and the integrity of defense systems and infrastructure. As a result, trust between the nations involved and their bilateral relations were undermined. The United States blamed Russia for the attack and imposed sanctions in response, increasing tensions between the two countries, following the line of thought of Alkhadra (2021).

In short, the 2019 SolarWinds attack was able to point out how interconnectivity can be harnessed to achieve strategic, political or military objectives, in a more accessible way and with the greatest possible reach compared to other traditional forms, such as direct warfare. In addition to strengthening and promoting, above all within the international community, the importance of cyber defenses and international cooperation in combating cyber weapons and the use of technologies in an underhanded manner, Liu (2022).

Another great example of how the lack of laws regarding the cyber space affects governments and international entities daily, is the South Korean phishing incident in july of 2023, where a government affiliated institution experienced an unprecedented scam that represents a huge loss for the country. The Institute for Startup Promotion, that operates under the Ministry of SMEs was attacked through a email phishing scheme, where the K-Startup Center aimed to help around 201 startups with an investment of 235 million USD, however, the business collaboration with Rainmaking requested an advanced payment of 135,000 via email, that was when an unauthorized phishing criminal gained access to the email between the companies, where the criminal meticulously altered the email address, allowing the responsible party to make the transfer to the wrong recipient, forfeiting over 100 million wons, showcasing the urgent need for increased vigilance and strengthened cybersecurity protocols in public organizations, per accordance with Seng (2023).

3.4 Resistance to full securitization due to advocacy and privacy concerns

With the aforementioned cases and studies, we can determine the importance of C.S. to the international scenario and politics, therefore leaving a mission to determine the legal frameworks and overall agreements to rule said area. To help this scenario, a group of distinguished scholars created the Tallinn Manual 2.0 on international law applicable to cyber operations, in cooperation with NATO and the Cyber Defense Centre of Excellence, containing 154 rules and about 500 pages on how applicable the international laws are in this context. Other than this, there have been many efforts from different actors to regulate or at least give some guidance on such matters, as an example, the Group Governmental Experts consensus report in 2015 endorsed by the U.N. General Assembly, where you can find a list of rules and guidelines on cyber activities that shall be followed by the voting states, not only that, but a "voluntary, non-binding norms of responsible state behavior".

In bestowal with Dr. Akande (2021), there is no need to create a new set of rules from scratch to include cyberspace, being that the UN charters, the Human Rights and International Law are applicable to the C.S. as well, however, it is a hard challenge to establish a multinational agreement, given each sovereignty, belief, laws and regulatory frameworks.

The sovereignty in the cyberspace refers to a state's right to control and regulate its online activities within its borders, including national security, economical interests, data management and many other rights, nonetheless, the key issues with this includes for instance, the jurisdiction of it, to determine which national laws shall be applied to internet activities that crosses borders, as well as data localization, considering that some countries require mandatory data from its citizens for security and privacy reasons. Another motive that clashes with the sovereignty is the content control, given that some states censor information and control the accessibility within their borders, which might raise concerns regarding free speech and human rights to other non according states.

The regulation of the international cyberspace can be noted trough the UN regulatory frameworks, consisting of charts, reports and treaties regarding recommendations and norms to shape behavior in this space, the Tallinn Manual, as previously mentioned, although it is not legally binding, has a large influence over this discussion, the Budapest Convention on Cybercrime (2001) being the first treaty looking to address cybercrimes and aiming to harmonize laws to improve the investigative techniques, the EU regulations such as General Data Protection Regulation (GDPR) to protect data, and the privacy of the european economic area (EEA) and its citizens, and the Detective on Security of Network and Information Systems (NIS Directive) that guidelines the obligations for most critical infrastructure operators and digital service providers.

4 INTRODUCTION TO THE FRAMEWORKS ADOPTED BY THE EU IN CYBERSPACE

4.1 Evolution of frameworks

Considering the notorious evolution of the EU approach on cybersecurity in the last decades, and the growing importance of safety in cyberspace, this section focuses on providing an overview on the main frameworks that helped shape the EU C.S. landscape.

Right at the start, in the early 2000´s, the EU´s main focus consisted on information security and data protection, with the adoption of Data protection directive in 1995, personal data security was harmonized with regulations across member states, allowing for ground rules to be established and later addressing how we would handle information in this upcoming digital world, in agreement with The European Data Protection Regulation (2013), "[it] laid down the general principles for the protection of personal data, but it left room for Member States to adapt some of its provisions, which led to fragmentation and inconsistencies in data protection laws across the EU." it became clear how the fast development of technology outpaced these provisions.

A big step forward was taken in 2004 with the creation of the European Network and Information Security Agency (ENISA), setting a coordinated effort in addressing cybersecurity issues. Evidently, the digital scenario was not as developed, resulting in limited action areas, but setting an important space for the following strategies and frameworks to be placed. According to the report, 81% of member states established a CSIRT, and the NIS Directive led to a 34% reduction in cyber incidents reported within critical sectors, ENISA (2022).

The digital policy in the European Union took a turn from 2009 to 2013, since cybersecurity started to be seen as a core element on the society, the Digital Agenda for Europe, launched in 2010, that represented a fraction of the broader Europe 2020 strategy, showcased the unsafeness of the digital world, resulting in measures to protect the critical infrastructures. Being a crucial part in maximizing the benefits of a thriving digital economy, their main focus was broadband expansion, data protection and boosting e-commerce, but the challenges presented included the speed and access to the internet that varied between states, and the quality of said access, EU commission (2014).

A huge influence on how European actors behave and legislate the C.S., was the Tallinn Manual, published in 2013 by NATO´s CCDCOE, Schmitt explains it:

> The Tallinn Manual is an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare. It was created by a group of international legal scholars and practitioners to clarify how the rules of armed conflict apply in the cyber domain (Schmitt, 2013, p. 7).

This shaped discourses in the cybersecurity law and helped setting different boundaries on state behavior.

After the introduction of the EU Cybersecurity Strategy in 2013, the organization´s vision for securing cyberspace was achieving cyber resilience, reducing cybercrime and developing a more comprehensive and coherent policy was laid clearer for all. The need for collaboration amongst international partners and the private sector was heavily commented, aiming to resolve the transnational nature of those cyberattacks.

Amongst the aforementioned strategy, it highlighted the Directive on Security and Information Systems (NIS Directive), considered the first fully comprehensive EU legislation in this area. It required member states to develop somewhat of a strategy on C.S. on a national level aiming on safety of data and systems, requested to strengthen relations and cooperation between countries, as well as new cybersecurity measures to be installed in critical areas such as energy, health, banking and transport. Information sharing was indeed another main focus on the NIS Directive, after the release of the Computer Incident Response Teams (CSIRTs), the cybersecurity incidents were heavily monitored beforehand, in attempts to stop, and properly reported, ensuring better coordination regarding the responses on those attacks.

The Cooperation Group, also formalized by the NIS Directive, brought light to issues such as lack of information sharing and coordinated responses on a large-scale, therefore, cross-border cooperation became formalized and the collective approach taken allowed for chances on addressing shared vulnerabilities in critical infrastructures, as seen in this passage, "[...] it plays a pivotal role in aligning national policies and ensuring that cybersecurity incidents are managed in a coordinated and efficient manner across the EU." (ENISA, 2019)

Notoriously, the threats we face nowadays have developed quickly, and their complexity grows daily, therefore the regulatory frameworks also developed with time, amongst the new directives published, the NIS 2 was introduced in 2020, and extends the scope of the original NIS Directive even further, covering sectors like public administration, manufacturing and digital infrastructure.

A milestone achieved within the EU was the adoption of the cybersecurity act in 2019, granting the ENISA a permanent mandate and expansion of its powers, turning it the central coordinating body for cybersecurity across the EU.

Focused on the governance of digital services, the EU has also released a series of ongoing initiatives aimed on cybersecurity capabilities, the Digital Services Act (DSA) and the Digital Markets Act (DMA) focus on provisions that can enhance the C.S. in online platforms and also digital marketplaces.

The Paris Call for Trust and Security in cyberspace (2018) is a relatively new initiative taken by the French president, Macron, in 2018 with the aim of setting common principles to address the current risks of cyberattacks and malicious activities. Established during the Paris Peace Forum, their 9 principles include protection of individuals and infrastructure, prevention of cyber attacks, promotion of responsible behavior from states and many others.

More than 100 entities signed the document, including Microsoft and other big-techs, however, states like China, USA and Russia have refrained from it. Seen as an extra file that compliments other existing agreements such as the Budapest Convention on Cybercrime and the Tallinn Manual, this initiative aims on complimenting gaps found and addressing states on their behavior and hopes to combat the proliferation of malicious cybertools.

4.2 Objectives of the frameworks

Considering each framework established in the EU in the past years has its own motivation, and has been guided by different objectives and importance, in the following subsection of this work, we can associate the main objectives with the previously mentioned frameworks.

The Data Protection Directive (1995) was the funding framework that opened the path for more regulations in the area, facilitating cross-border data transfers and setting a pattern for laws between member states. It´s main goal was achieved, since the focus was safeguarding personal data and privacy, they ensured individuals´control over their personal data. Its principles include data minimization, storage limitation, right to rectification and to object, with the supervision of national data protection authorities.

The European Network and Information Security Agency (ENISA, 2004), helped improve the C.S awareness and practices, it focused on coordination the C.S. efforts across the EU. They successfully provided member states with support and expertise on cyber matters, enhancing cooperation and information exchange, developing a bigger culture of security awareness among stakeholders.

The Digital Agenda for Europe (2010) helped set guidelines for the digital economy, while increasing the visibility of cybersecurity issues in economic policies, they successfully promoted a secure digital environment while protecting critical infrastructures from Cyber threats, expanded internet access and security, while promoted e-commerce and data protection, what helped with encouraging the development of a digital economy.

The Tallinn Manual (2013) influenced international discussion regarding cyber warfare and statal behavior on C.S., its publication helped on limiting the laws and clarifying the rules of armed conflicts, promoting more responsibility and accountability, although non-binding, the manual set unprecedented ground rules for future agreements, according to statistics. A survey indicated that 59% of international legal scholars acknowledged the Tallinn Manual as a pivotal reference for understanding cyber conflict, Kessler (2013).

The EU Cybersecurity strategy (2013) allowed for a unified approach on C.S. and highlighted the need for collaboration amongst stakeholders. It helped set a more comprehensive framework and a collaboration between private and public sectors.

The NIS Directive (2016) was the first EU-wide legislation with its main focus on system security and cybersecurity strategies, aiming on preparedness and incident responses, required member states to adopt a set of measures aforesaid, and overall facilitate information sharing and cooperation. The NIS 2 Directive (2020), on the other hand, became a central position, improving the cyber governance game and established a stronger framework.

5 ANALYSIS OF EU POLICIES AND STRATEGIES

5.1 EU cybersecurity strategy

After centralizing and coordinating efforts to address the challenges in cybersecurity, ENISA in 2004, increased cooperation in this area, expanding its action path with the EU's security defense policies. Moreover, the trajectory of C.S. was changed in 2013 with the publication of EU Cybersecurity strategy, being a comprehensive approach of resilience of information systems, critical structures and digital services, placing an important emphasis on building a cyber shield for the EU through public-private cooperation, greater cybersecurity investments, and increased collaboration between EU institutions and member states.

The NIS directive also contributed to the growth in this area, establishing risk management and incident reports, defining the action and obligations of Operators Essential Services, and providing digital services as cloud computing. It helped to harmonize cybersecurity measures and led to an increase in transparency and accountability, however, some States still struggle to align the requirements from the directive since they present limited resources or differ in its national priorities. During the COVID-19 pandemic, the NIS Directive has proven crucial since many attacks focused on the healthcare system, the directive required the implementation of stronger measurements and faster reporting of incidents, as mentioned by the World Health Organization,

> Consider, for example, recent attacks on healthcare systems during the COVID-19 pandemic that brought hospitals to their knees and limited their ability to provide critical care for their patients. The NIS Directive paved the way for a significant change in mindset, institutional, and regulatory approach to cybersecurity in many Member States (WHO, 2024).

The EU Cybersecurity strategy, updated in 2020, guidelines EU´s posture in the C.S., amongst other initiatives created, there is the european Cybersecurity Competence Centre (ECCC), initiatives that foster innovation in technology and reduce the dependence on non-EU providers, enhancing their sovereignty. With the Cyber Crisis Liaison Organisation Network (CyCLONe) they can coordinate swiftly and respond effectively to the large-scale incidents within EU members, to unify and easen the approach and response to attacks.

5.2 Transnational cooperation and alliances

Undoubtedly, transnational cooperation plays an important role in addressing global challenges, as the EU navigates on the geopolitical landscapes, it actively collaborates amongst other international organizations aiming to enhance security, foster stability and promote human rights.

The EU-NATO cooperation has evolved over time, having its start in 2003, after the 2016 Warsaw Joint Declaration and the 2018 Brussels Joint Declaration, and operating in different spheres, where NATO's main goal is economic integration, some main areas of cooperation are the security defense, joining efforts to coordinate crisis management, share intelligence, military exercises such as the ALTHEA one in Bosnia and Herzegovina to peacekeep. Cybersecurity wise, they have big programs together on capacity-building and joint-response, like the technical arrangement that include real-time intelligence sharing, best practice sharing, and industry partnership emphasizing collaboration with industry stakeholders. Showcasing their commitment to collective defense, in response to Russia's illegal invasion of Ukraine, In January 10th of 2023, the EU and NATO released a joint condemnation, unifying and highlighting their commitment to Euro-Atlantic cooperation and security; It also contains a strategic partnership in security approach, playing complementary, coherent and mutually reinforcing roles to help international peace, EUROPEAN COUNCIL, (2023).

Different cooperations with the EU include Interpol and its help provided among law enforcement agencies worldwide, the European Cybercrime Centre (EC3) that supports member states in combating online criminal activities with operational support, and many other entities such as The council of Europe, where they both work around the Budapest Convention to prosecute crimes.

5.3 The role of ENISA (European Union Agency for Cybersecurity)

ENISA was established in 2004 with the goal of enhancing cybersecurity in the EU, based in Greece, they collect data on previous incidents and publish reports and threat assessments to inform EU institutions regarding current cyber threats and trends. Other than providing guidelines, and giving training programs for the public and private sectors, they also contributed to the implementation of the Cybersecurity Act and the NIS Directive.

Serving as a main organism for cyber threats monitoring, ENISA collects data on cybersecurity from both private and public sectors, publishing their annual Threat Landscape Report. In the 2024 Threat Landscape Report we can see the breakdown of analyzed incidents by threat type, and notably DDOs/RDO and Ransomware are the most common ones, with an average of 66.89%. Evasion techniques such as LOTs or Living off Trusted Sites are growing each year more, where hackers use trusted sites and legitimate services to avoid being detected and hide, adopting commodity tools, dual-use softwares and open-source softwares, ENISA (2024). Many other tools help criminals maneuver in the cyber world, such as the spike in usage of AI tools to co-author scam emails, IABs, mobile banking trojans and others.

Geopolitical crises continue to directly affect cyber malicious operations, state conflicts and international disputes that are often brought to the C.S. as a way to showcase power, disrupt rivals and achieve goals without engaging in conventional warfare. During said tensions, a state might sponsor or tolerate cyberattacks towards rivals, such as NotPetya in 2017 attributed to Russia during the crisis in Ukraine, which consisted of Asymmetric warfare, since Ukraine presented fewer resources to launch or protect themselves, causing a disruption of infrastructure like electricity grids and government systems.

This demonstrates how cyberspace has become an arena for geopolitical conflicts, where they leverage vulnerabilities in information and communication systems to achieve their plans. In agreement with the neoliberal institutionalist points of view, states should have a will to cooperate through institutions that regulate this area and establish norms for behavior and responsibility, since this reduces uncertainty and facilitates cooperation, providing benefits to all parties involved. As an example of institutions we can see the EU and NATO, that facilitate the cooperation by fostering communication sharing, a sense of collective defense and risk reduction. Therefore, with the given information regarding neoliberal institutionalism and geopolitical cyberthreats, ENISA can be seen as a core tenet in helping coordinate regulations and responses during cyberattack stemmings.

Overall, ENISA also helps understand what areas are the main focus of attacks and why, understanding the motivation behind an incident is crucial in determining what their aim is, with the main objectives being Financial Gain, Espionage (gaining information on Intellectual property, classified data …) , Destruction with irreversible consequences and Ideological (backed up with a line of thought that usually constitutes hacktivism).

6 ANALYSIS OF NATO´S POLICIES AND STRATEGIES

6.1 NATO Cybersecurity Strategy

Ensuring the alliance´s ability to deter and respond to cyber threats, NATO has an approach focused on collective defense and the integration of C.S. into the security agenda. Its first Cyber Defense Policy, in 2008, emphasizes the protection of networks, that in NATO´s Enhanced Cyber Defence Policy, adopted in 2014, recognizes that cyberattacks could trigger the 5th article of NATO Charter (collective defense), possibly seen as an attack on all member states and leaving an opening for a collective response. A leap on development came with the Wales Summit in 2014, where leaders declared the cyberspace as a domain of operations, meaning it can be seen as similar to land, sea, air and space domains, highlighting the commitment to its capabilities in cyber defense and engaging in a broader defense plan.

In accordance with NIS Directive and their security measurements, NATO members take a similar approach and balances off of NIS, where focusing on incident reports and risk management helped NATO share its issues and vulnerabilities, leading to improvements in collective awareness and response methods.

The Collectiveness of NATO's defense mechanism ensures that member states can collectively and properly defend against cyberattacks, having the help of Cyber Rapid Reaction Teams (CRRTs), often deployed to assist members in significant incidents.

Furthermore, similar to other frameworks previously mentioned from other entities, such as information sharing and intelligence gathering, cooperation amongst entities as the EU and capacity building, NATO has been a pillar in establishing a common framework across the European Union and collaborative cyber defense efforts.

6.2 Transnational cooperation and alliances

Transnational cooperation plays a major role in cyberspace, helping address multifaceted challenges imposed by cyberthreats, the EU often collaborates with other actors such as NATO and the Council of Europe to ensure an unified response in this borderless issue.

The shared objectives of NATO and EU stand on common objectives between them, like enhancement of security and stability, frameworks for said 'partnership' include prioritization of rapid exchange of threat intelligences in order to bolster collective defense, joint exercises amongst similar teams as Computer Incident Response Capability (NCIRC) at NATO and Computer Emergency Response Team (CERT-EU) at the EU, capacity building with similar instruments on cyber incident simulations like EU´s Cyber Europe and NATO´s Cyber Coalition and policy alignment with previously mentioned policies like the Cyber Defense Policy for NATO and NIS Directive for the EU.

In collaboration with the Council of Europe, the first binding international treaty for cybercrime, the Budapest Convention on Cybercrime released on July 1st 2004, is fully supported by the EU. The criminalization framework outlaws specific activities across all member states, such as unauthorized access to computers and systems (hacking), unauthorized tampering with data or systems, such as malware, usage of computers to commit fraud, phishing and online scams, and distribution or possession of child pornography. The tools and methods for investigations and prosecution may include powers granted to authorities to investigate cybercrimes, including seizing computer data, preservation and securing electronic evidence related to any crime, while including provisions for some countries for mutual help in investigations, prosecutions, and extradition of cybercriminals. The harmonization of this makes it easier for states to address and punish the crimes and its doers.

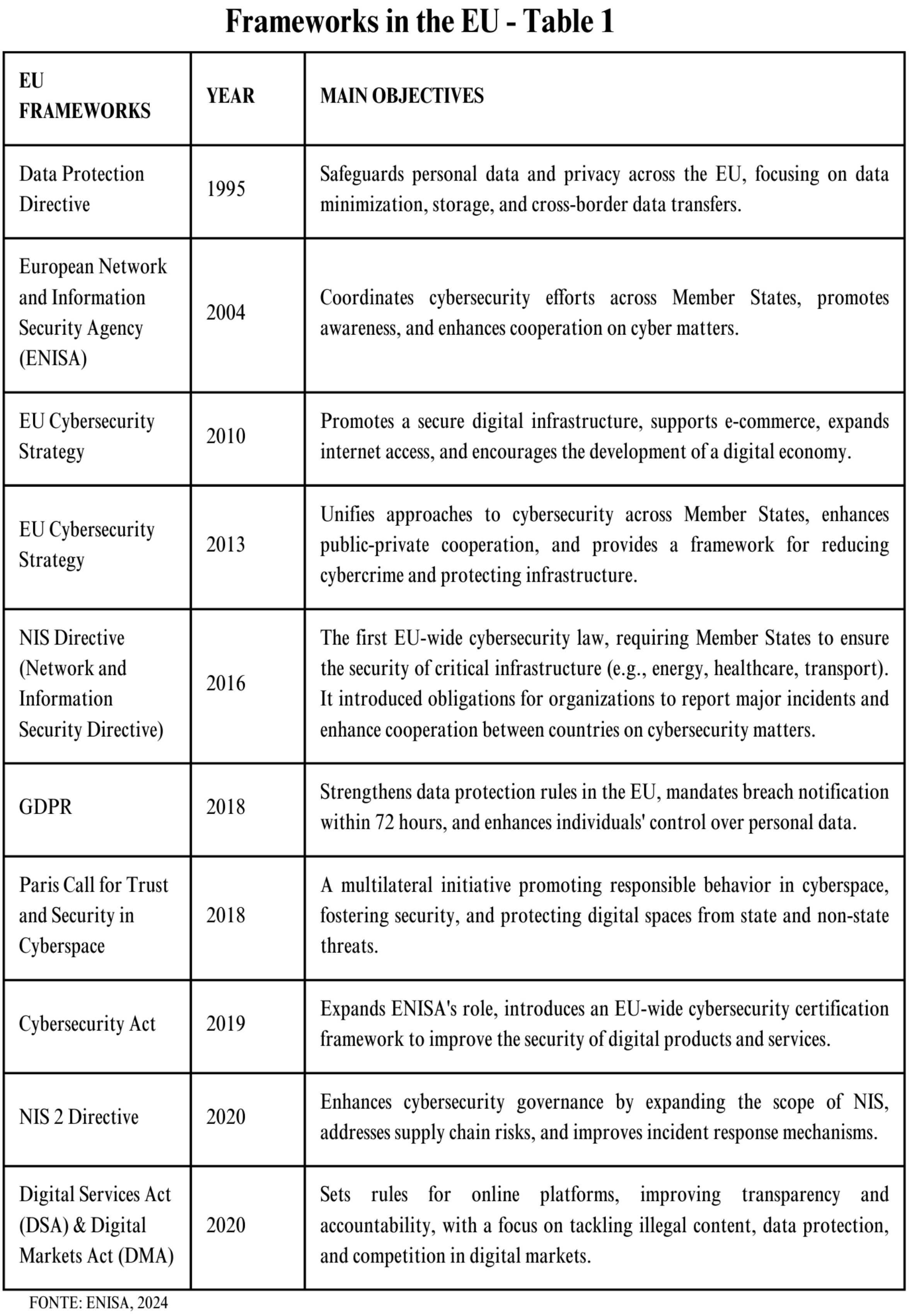
Some key points of it include the criminalisation of conduct that range from illegal access, data and systems interference, procedural powers to investigate cybercrime and secure electronic evidence in relation to any crime, and efficient international cooperation between parties, as listed on the EU law, (2023). As well as in the additional protocol 2, aiming to enhance international cooperation they feature, new legal basis that allow for a direct request to registrars in other jurisdictions for obtainment of domain name registrations information, allowing direct orders to service providers to obtain subscriber information even in other jurisdictions, also obtaining subscriber information and traffic data through government-to-government cooperation, and expedited cooperation and joint investigation teams in emergency occasions.

7 EFFECTIVENESS INDICATORS

7.1 Main Cyber Attack Incidents

Amongst the most notorious cyber attacks registered in recent years, both public and private sector have been affected in high-profile incidents, such as NotPetya in 2017, WannaCry in 2017 and Solar Winds in 2020, disrupting critical infrastructures and essential services in the European Union, representing great financial loss and emphasizing the need for stronger cybersecurity measures.

Table 1 - Frameworks in the EU



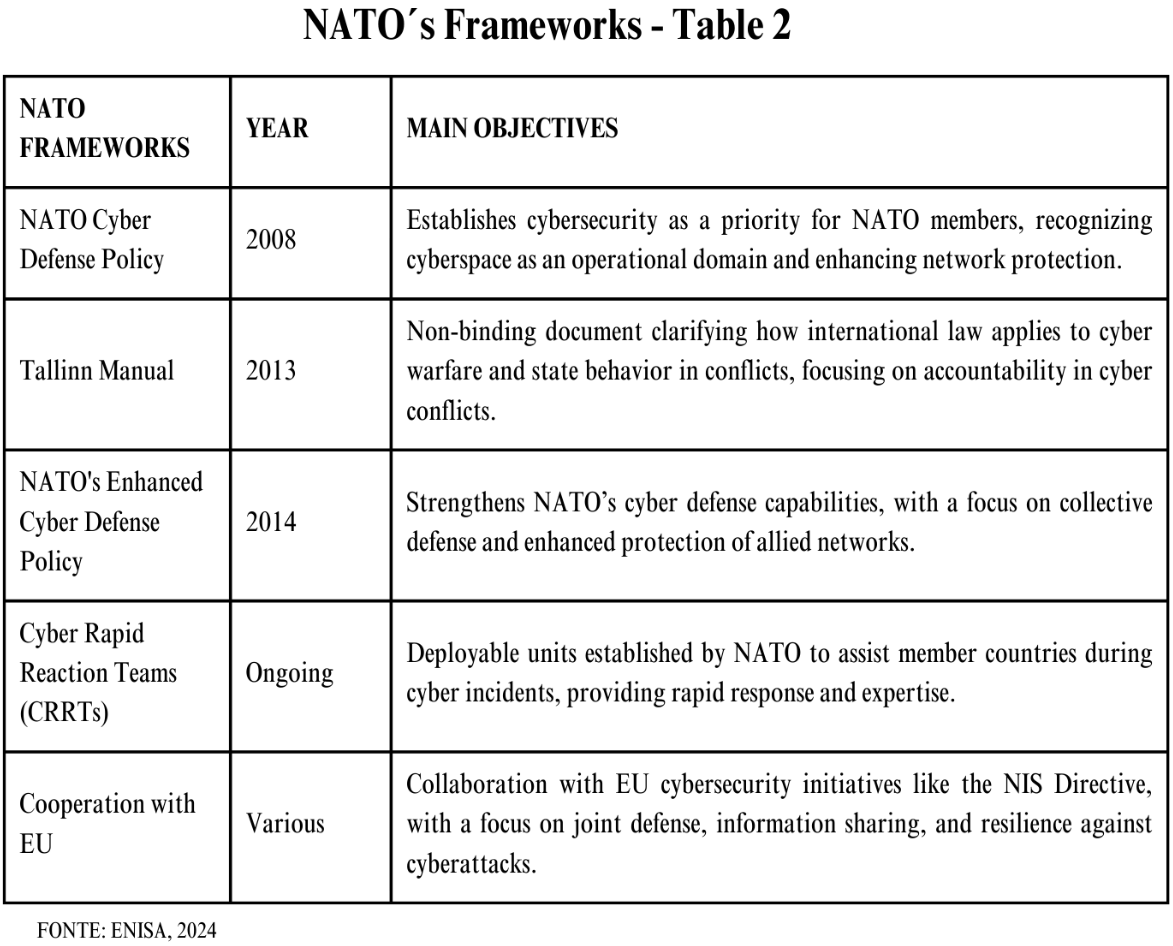
Frameworks in the EU - Table 1

EU FRAMEWORKS	YEAR	MAIN OBJECTIVES
Data Protection Directive	1995	Safeguards personal data and privacy across the EU, focusing on data minimization, storage, and cross-border data transfers.
European Network and Information Security Agency (ENISA)	2004	Coordinates cybersecurity efforts across Member States, promotes awareness, and enhances cooperation on cyber matters.
EU Cybersecurity Strategy	2010	Promotes a secure digital infrastructure, supports e-commerce, expands internet access, and encourages the development of a digital economy.
EU Cybersecurity Strategy	2013	Unifies approaches to cybersecurity across Member States, enhances public-private cooperation, and provides a framework for reducing cybercrime and protecting infrastructure.
NIS Directive (Network and Information Security Directive)	2016	The first EU-wide cybersecurity law, requiring Member States to ensure the security of critical infrastructure (e.g., energy, healthcare, transport). It introduced obligations for organizations to report major incidents and enhance cooperation between countries on cybersecurity matters.
GDPR	2018	Strengthens data protection rules in the EU, mandates breach notification within 72 hours, and enhances individuals' control over personal data.
Paris Call for Trust and Security in Cyberspace	2018	A multilateral initiative promoting responsible behavior in cyberspace, fostering security, and protecting digital spaces from state and non-state threats.
Cybersecurity Act	2019	Expands ENISA's role, introduces an EU-wide cybersecurity certification framework to improve the security of digital products and services.
NIS 2 Directive	2020	Enhances cybersecurity governance by expanding the scope of NIS, addresses supply chain risks, and improves incident response mechanisms.
Digital Services Act (DSA) & Digital Markets Act (DMA)	2020	Sets rules for online platforms, improving transparency and accountability, with a focus on tackling illegal content, data protection, and competition in digital markets.

FONTE: ENISA, 2024

Fonte: ENISA, 2024

Table 2 - NATO´S Frameworks



NATO´s Frameworks - Table 2

NATO FRAMEWORKS	YEAR	MAIN OBJECTIVES
NATO Cyber Defense Policy	2008	Establishes cybersecurity as a priority for NATO members, recognizing cyberspace as an operational domain and enhancing network protection.
Tallinn Manual	2013	Non-binding document clarifying how international law applies to cyber warfare and state behavior in conflicts, focusing on accountability in cyber conflicts.
NATO's Enhanced Cyber Defense Policy	2014	Strengthens NATO's cyber defense capabilities, with a focus on collective defense and enhanced protection of allied networks.
Cyber Rapid Reaction Teams (CRRTs)	Ongoing	Deployable units established by NATO to assist member countries during cyber incidents, providing rapid response and expertise.
Cooperation with EU	Various	Collaboration with EU cybersecurity initiatives like the NIS Directive, with a focus on joint defense, information sharing, and resilience against cyberattacks.

FONTE: ENISA, 2024

Fonte: ENISA, 2024

The public sector, including national government and sectors of if have been greatly impacted by the WannaCry ransomware attack, having a big effect in the UK's healthcare system (NHS), causing the cancellation of multiple health procedures and surgeries, exemplifying the need to boost the cyber defense in all areas. In the private sector, the damages does also compare, as in the attack NotPetya, several companies like Maersk, one of the biggest shipping enterprises, was partially shut down and had a tremendous financial loss, in accordance with Greenberg (2018).

This attack exploited the EternalBlue failure in Windows, that had been partially patched by Microsoft but not by specific organizations, being the entry point for hackers, as well as the Mimikatz, that enabled the spread to go further and faster within networks, while stealing credentials and accessing systems even if patched against EternalBlue. This spread from Ukraine and across Europe, affected critical infrastructures, logistics and energy sectors, however, some frameworks installed helped to control said issue, the NIS Directive (2016), recently released at the time of the attack, helped EU Member States on adopting certain strategies that settled the baseline security standards on matters like incident reporting (quicker communication on affected institutions, helped understand the scale of the attack), information sharing (more collaboration and sharing of threat intelligence for a faster response), but it also presented a few limitations since it had been installed for a short period of time, a few sectors had not incorporated the guidelines yet, resulting in a less prepared section, that led to a rapid spread of the malware.

However, given the main goal of the attack, destroying the system while wiping the Master Boot Record (MBR) and making data recovery impossible by encrypting the Master File Table (MFT), this led to massive operational disruptions in the affected companies, showcasing the real goal to be a destructive attack, not a ransome one, what wasn't comprehensively approached in the NIS Directive and initiated the need for a broader regulation and protocols to be followed. With the lack of guidance from the NIS, the EU and other countries invoked diplomatic tools and sanctions against Russia, since it had been pinned as the main actor in the attack and highlighted the need to address and better stipulate state-sponsored cyberattacks in this geopolitical level.

The WannaCry attack in 2017 can be considered one of the most damaging ransomware attacks to happen, exploited vulnerabilities in the Microsoft Windows, infecting systems through a worm, and after its dissemination, a ransome in bitcoins was requested. Also exploiting the EternalBlue, a vulnerability present in Microsoft´s Server Message Block (SMB) protocol, that was leaked by the group Brokers in April 2017 after the NSA was hacked, it encrypted files on individual computers which led to the extortion of victims. The attack was attributed to North Korea´s Lazarus Group doing´s, being considered a state sponsored attack, the response provided by Microsoft´s Patch (MS17-010) wasn't largely used, causing an easier access, and the release of a few other emergency patches for outdated systems took place. Regarding the frameworks, once again the NIS Directive t was used, but seen by the previous attacks that year, the GDPR came into the scene after this attack, in 2018 this newly developed protocol suggested a stronger security measure with incident reporting being mandatory, Sanger (2017).

In order for cyber attacks to be detected, it is necessary to constantly monitor the network, as well as safeguarding it with a highly developed network and systems that allow an adequate firewall for the desired use and protection, exemplifying this, the SolarWinds attack in 2020 is a representation of high sophistication in the cyberworld by the attackers, compromising the systems of a third-party software provider (solarwinds itself), hackers introduced a malware (SUNBURST) into a software (Orion) update, meaning that whenever consumers updated or downloaded their products, they would automatically be infected and compromised, Center of Internet Security (2021)

The attack allowed hackers full access to the computers of companies using SolarWinds, including the White House, the Pentagon and several other US agencies. It is believed that they had the support of Russian intelligence agencies, but the attack has not been claimed by any country, however, this is a well-known Russian tactic in the hope of preserving warfare and keeping countries considered hostile "under control" (Coco, 2022).

Companies such as FireEye and Cisco had been heavily impacted too, this showcased the global impact of an attack, therefore using internationally known measures like the GDPR that stipulated the report of data breaches and helped organizations to respond quickly and comply with the legal obligations. The Cyber Diplomacy Toolbox (2017) accessed other international bodies to impose sanctions on Russia, as well as the CERTs (Computer Emergency Response Teams) that analyzes the attack and its impacts while coordinating responses across affected organizations. This attack led to the development of the NIS 2 Directive, expanding the scope of cybersecurity legislations and supply chain risks.

The 2022 Cyberatack on Montenegro, targeting the country's government and critical infrastructure, showcases how a non-EU country (at the time) but a NATO member, can take advantage of set frameworks and work together in incidents. In August 2022 the country was hit by a sophisticated attack, being attributed to state-sponsored actor by the Russian government, being a member of NATO allowed the country to call on a collective cybersecurity framework, deploying NATO´s cyber response team to help mitigate the damage, and although the 5th Article was not invoked, a technical assistance was provided through the CCDCOE on recovering the critical infrastructure, NATO CCDCOE (2022). The partial alignment with the NIS directives also helped guide the response and ensure the functioning of the essential services, as well as the information sharing and coordination by ENISA. Being also a supporter of the Paris Call for Trust and Security in Cyberspace, Montenegro also endured the facilitation of broader diplomatic and cyberdefense cooperation during the incident

Considering the aforementioned cases and the protocols that took place, is clear the need for better preparedness specially in critical sector such as the NHS that should have upgraded their operating systems and implemented stronger defense mechanisms, also shadowing the need to enforce the NIS Directive quicker and more comprehensively, including a focus on supply chain security, partially included in the NIS 2 but still presenting a gap in addressing certain issues. It lacked specific provisions for third-party vendor management, which would require companies to access the security of their software providers. The failure to implement measurements and updates, reflecting the poor cyber hygiene and lack of proactive management, as well as the outdated systems used, turned them into susceptible targets.

The overall limitations presented, such as lack of management or specific inclusions in frameworks, failure to enforce timely software updates, lack of supply chain security, partial implementation of directives and lack of enforced power while holding state actors accountable in a meaningful way, reveals a significant weakness and lack of thoughtful creation to effectively handle said issues.

7.2 Effectiveness Indicators

For this section, the metric used to evaluate the effectiveness of EU´s cybersecurity will rely on qualitative and quantitative data in order to assess the attack rates, infrastructure resilience and incident response capacity. Using different incident reports from up until 2024, frameworks will also be considered, like the NIS and NIS 2 Directive, GDPR, NATO's cyberdefense mechanisms and the other aforementioned ones.

The analysis of attack rates between 2016 until 2024 comprehends the most important and pivotal attacks suffered in such matters, where before the frameworks were implemented, in 2016, there was an increase in attacks on critical infrastructure. The attacks we previously discussed such as NotPetya (2017) and WannaCRy (2017) opened a few vulnerabilities in the healthcare system, finance and transportation system. The response capabilities in those areas were limited, and the frameworks were either non-existing or very minimal, therefore the EU ENISA Threat Landscape Reports from 2017 shows a significant rise in ransomware attacks, and around 230.000 systems were impacted in some way by attacks like WannaCry and NotPetya, that led to a $10 billion global loss.

Before the implementation of frameworks like the NIS Directive, in 2016, attack rates had a sudden rise, specially on critical infrastructures, the number of attacks in these sectors such as healthcare and energy showed the lack of comprehensive defense mechanisms in the EU. Post a few framework implementations, from 2018 to 2024, there was a significant decrease in attacks, where the decline of reported cyberattacks on critical areas lowered around 15 to 20% from 2017 to 2023. The GDPR, in 2018, mandated a 72 hour breach notification, which led to an increase in reports initially, showing more transparency rather than an actual rise in attacks.

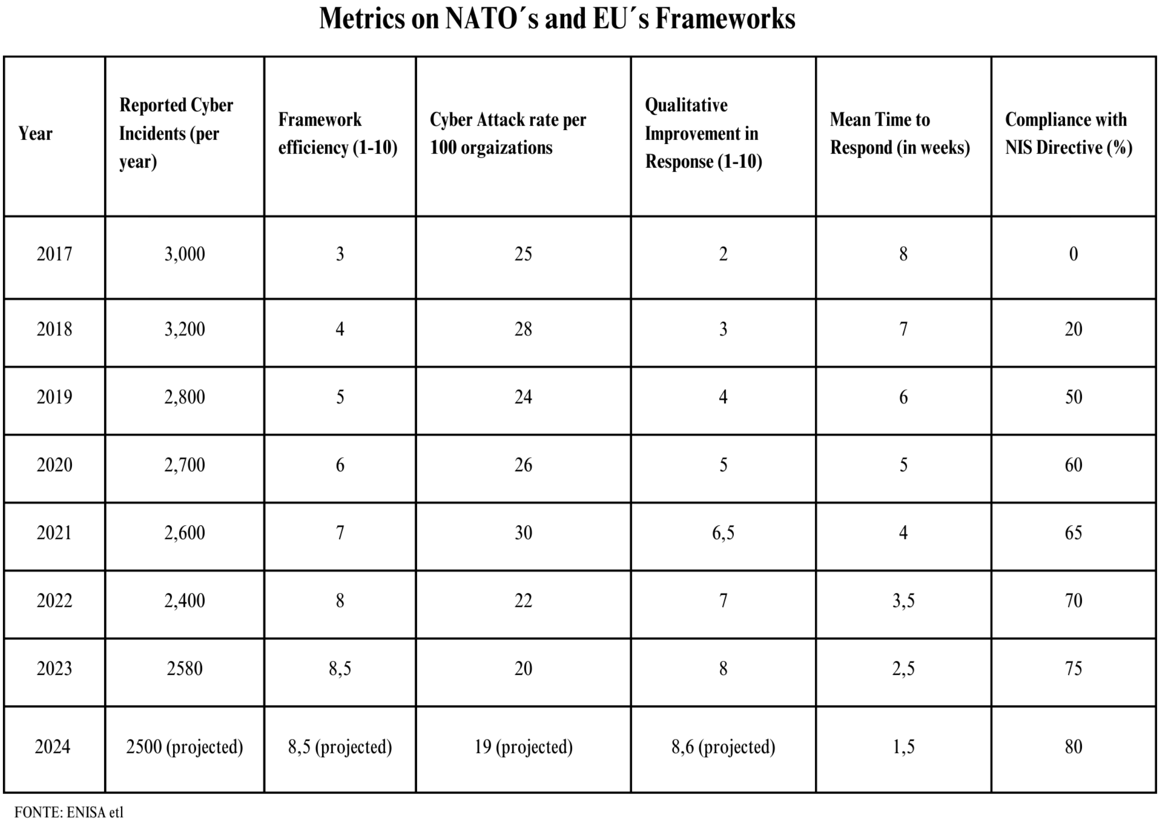
The effectiveness of frameworks on attack rates exhibits a slowdown in critical sectors, the ones covered under the NIS Directive saw a 30% drop in these successful attacks by 2023, introducing an efficacy in essential services after the frameworks. However, supply chain attacks like the breach from SolarWinds in 2020, describes howm some vulnerabilities not covered by the NIS led to further reforms for the NIS Directive 2, now covering supply chain security and cloud providers, partially addressing this gap. Although we had a decline in traditional ransomware attacks, the advanced persistent threats (APT´s) and supply chain attacks surged by 25% from 2020 to 2024, ENISA (2023), for the lack of more comprehensive frameworks to address it.

The infrastructure resilience will be based on a quantitative and qualitative analysis, where the key metrics are the compliance with the NIS Directive, that shows more than 75% of organizations in the critical sector had implemented the measures required under the directive, an improvement from the previous 50% compliance in 2019. The energy sector showed an even higher compliance, with 95%, unveiling better preparedness.

The impact of attacks on services in 2017, like NotPetya, led to long disruptions, and by 2023, the recovery time for a cyberattack had decreased to around 1 to 3 weeks for essential services.

When evaluating the infrastructure and resilience, the vulnerabilities seen before the NIS, in areas corresponding to healthcare, transportation and other means were inappropriately protected, seen by the WannaCry´s impact on the UK's health system, facing weeks of operational disruptions. After the implementations, organizations started introducing incident response plans, and a more prepared disaster recovery mechanism, allowing for a faster recovery on cases of major attacks, as seen in the Montenegro Cyberattack in 2022.

The Incident Response Capacity, using the Mean Time to Detect (MTTD), shows that in 2017 it took 6 months to do so, and in 2023 it takes 1 to 3 weeks, all thanks to the incident reporting and coordination shown amongst guidelines like the Computer Security Incident Response Team (CSIRTs). The reporting of data breaches since the installment of the GDPR in 2018, showed an increase to over 160.000 reports on data breaches between 2018 and 2023, ENISA (2023).



Metrics on NATO´s and EU´s Frameworks

Year	Reported Cyber Incidents (per year)	Framework efficiency (1-10)	Cyber Attack rate per 100 orgaizations	Qualitative Improvement in Response (1-10)	Mean Time to Respond (in weeks)	Compliance with NIS Directive (%)
2017	3,000	3	25	2	8	0
2018	3,200	4	28	3	7	20
2019	2,800	5	24	4	6	50
2020	2,700	6	26	5	5	60
2021	2,600	7	30	6,5	4	65
2022	2,400	8	22	7	3,5	70
2023	2580	8,5	20	8	2,5	75
2024	2500 (projected)	8,5 (projected)	19 (projected)	8,6 (projected)	1,5	80

FONTE: ENISA etl

Fonte: ENISA etl

As demonstrated in the chart on insert 3, key metrics are shown from 2017 to 2024, divided between EU and NATO´s frameworks, with a focus on cyber incident reports, framework efficiency and other metrics taken from previous ENISA reports such as the Investments Report, Threat Landscape Report, and Official Documents from respective frameworks.

As seen in the chart presented, it is noticeable the advances in the frameworks from 2017 to 2024, demonstrating the growing efficiency of properly reporting incidents, following the NIS Directives and adequate response mechanisms, highlighting the coordinated efforts from the EU and NATO and its allies, and the pivotal roles of their established rules and recommendations.

7.3 Impact on Member States

The implementation of directives such as NIS and GDPR by Member States largely influences the effectiveness of the EU Cybersecurity frameworks, and the disparity in the usage of said regulations impacts significantly the overall cybersecurity posture of the Union.

High performing countries such as Estonia, who is an example of success rate in implementing cybersecurity frameworks, since after its attacks suffered in 2007, had a heavy investment into integrating C.S. in their national security strategy. By 2022, the country had 100% compliance with the NIS Directive and strong partnership with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE).

France can be considered another strong compliant country with the EU regulations, developing sectoral CSIRTs and heavy investments in defense in cyber areas, the French National Cybersecurity Agency (ANSSI) launched countless initiatives to coordinate efforts between public and private sector, like Cyber Campus. However, many countries still struggle with implementing the full scope of the directives, like Greece and Portugal, with C.S. still being a developing field, the compliance rate on critical sectors in these countries represents around 50% in 2021, in comparison with more advanced countries that have an average of 80 to 90%,

This disparity in the applicancy and administration of frameworks intervenes in the overall success rate of the EU, with multiple factors contributing to this issue, the main ones are the economic resources a country has, the political will and commitment to it, for instance, Finland and Denmark have it incorporated into their broader national defense strategy, while others consider it a secondary issue. The public to private collaboration also facilitates a faster use of the measures, seeing if a country has a weak cooperation, the process is fragmented and slower.

Countries that fall behind in the fulfillment of the directives like NIS, become weak links, which exposes the entire Union to risks and threats from cyber criminals and state-sponsored attacks, looking to exploit this gap. Therefore, collective responsibility in cybersecurity is essential to avoid cascade effects across the EU, especially if evolving cross-border critical infrastructure such as energy and telecommunication.

After the introduction of the NIS 2, efforts to standardize the implementation of frameworks have been strengthened, while expanding the scope of sectors that shall be covered with a stricter requirement, the directive aims to close this gap seen between high-performing countries and the ones not so advanced in compliance.

8 CONCLUSION SECTION

8.1 Summary of Findings

In this summary of findings, is noted that the implementation of EU Cybersecurity frameworks such as the NIS Directive in 2016 and its successor, settled a turning point in the development of policies, providing a new viewpoint for the legal frameworks on the protection of critical infrastructures, while improving incident responses.

Set out to examine the extent in which the cybersecurity frameworks adopted by the EU have proven itself effective in enhancing cyber resilience, likely influencing the global response to cyberattacks. Through the analysis of empirical evidence, several key trends, challenges and cases of success, this shall reflect the ongoing state of governance in this merit in the Union.

The analysis shows that compliance rates have increased lightly, with over 75% of organizations in critical sectors implementing the NIS measures by 2023. In the energy sector the compliance is higher, reaching around 95%, showcasing the uptake in readiness for situations.

The response received on major cyberattacks like the ones mentioned in this article, exposes the vulnerabilities of critical infrastructure, specially in healthcare and transportation sectors before the implementation of frameworks. By 2023, the mean time to detect and respond to cyber incidents decreased, from 6 months in 2017 to 1-3 weeks in 2023.

The GDPR´s role in Data Protection and Breach Reporting was considerable, with around 161.000 data breaches reported between 2018 and 2023, this directive promoted transparency and accountability in practices across the EU.

It also impacted international responses to cyberattacks, with initiatives such Paris Call for Trust and Security in Cyberspace, the EU has taken a central role in promoting responsible state behavior. Enhancing the collective capabilities, the collaboration between the EU and NATO has proven itself crucial, as well as the Tallinn Manual in providing clarity on the application of international law in cyber conflicts.

Although said directives have proven itself useful in the past years, there are still gaps that need to be addressed regarding the supply chain security, for instance, during the solarwinds attack, the third-party vendors were not comprehensively covered under the original NIS framework, exposing the need for a better oversight on it, expanding the scope to cover entities and to include cloud providers while managing this service providers, what would effectively address this risks.

Presented as one of the main issues in cybersecurity, addressing state sponsored attacks and attributing state-backed attacks is challenging, especially holding them accountable. This limitation explains the need for a better and more robust international cyber diplomatic framework, as partially addressed in the Paris Call for Trust and Security in Cyberspace but still lacking deep legislation on this matter. As seen through the lens of Neoliberal institutionalism, multilateral agreements and institutions can help on the creation of mechanisms to better attribute accountability, however there is still a lack of mechanisms to do so efficiently, therefore this issue stems from the weakness presented by existing institutions in creating a binding international agreement that would effectively hold states accountable for those cyber agressions.

Although notable progress has been made in cyberspace, there are still breaches remaining, such as the disparity in compliance among member states, challenges in addressing these emerging threats like AI-driven attacks, and the implementation of a comprehensive framework that is yet to be developed.

8.2 Final Assessment of Hypothesis and Recommendations

As the previous sections of this article explain what the frameworks include and the overall effectiveness seen in real life cases, is noticeable that it has been effectfull on fostering a more secure and coordinated response, and also significantly improved cyber resilience, however there are major gray areas that allow for criminals to maneuver, and this need to be addressed quickly.

The issues such as disparity in implementation, supply chain vulnerabilities, accountability in state sponsored attacks and efficiency of measures in strikes, turn the validation of ‘EU frameworks fostering a more coordinated and secure international response’ partially truthful, as there is a lot of evolution and expansion to be done on these frameworks in order to tackle this new and emerging disputes in the digital age.

Based on the findings of this thesis, several recommendations can be made in order to address these issues in the frameworks, such as an enhanced support for lagging member states, with incentive programs to help these members like Greece and Portugal to improve their infrastructure, with financial aids and technical expertise. Another point on this could be the inclusion of penalties for non-compliance with mechanisms like the NIS 2 Directive, monitoring Member State´s adherence to these standards. Mandating benchmark reports EU-wide would also facilitate the understanding of their progress and foster a healthy competition to achieve full compliance.

Many other specific issues need to be targeted in a specific framework, like addressing the supply chain vulnerabilities, by requiring a mandatory vendor assessment, and introducing a cybersecurity certification for software providers and/or third party-vendors handling sensitive data or providing critical infrastructure services. The key to achieve a future stability and proper cyber crisis management is ensuring cooperation between NATO, EU and international institutions, broadening NATO´s role in cyberdefense, creating a joint EU-NATO cybersecurity task force, for incident response groups and intelligence gathering and sharing. The public and private sector are a main challenge in this, seeing that they should have a better communication and information sharing mechanism to facilitate faster responses and collective defense mechanisms.

Developing a better international cyber norm to address problems like the lack of accountability for state-sponsored attacks, and establishing a binding agreement globally on cyber warfare are of utmost importance to tackle emerging threats. The creation of a new treaty can be challenging and not well received, therefore building up on frameworks already established like the Paris Call for Trust and Security in Cyberspace, can help institute clear consequences and possible sanctions /legal actions to be taken.

In conclusion, the EU´s cybersecurity frameworks have been effective in providing cyber resilience and response capabilities, where the directives like NIS and NIS 2 laid an important foundation for protecting critical infrastructures. The GDPR was a game changer on transparency and incident reporting, and the combined efforts of NATO enhanced the collective defense and improved multilateral cooperation. However there are slots to be filled like the ones mentioned above, consequently, future efforts shall focus on developing international agreements and evolving with the cyber threat landscape that is constantly changing, with continued innovation and collaborations in this area, ensuring long-term stability in this digital age.

CONCLUSION

Trought this article, aimed at understanding the frameworks imposed on cyberspace, especially within the European Union, the international responses are shaped by it and directly influence our daily lives. This research showcases that cyberspace is a profusely complex and transnational area, challenging the traditional and conventional mechanisms used, as well as the conceptions of sovereignty and security. This fluid characteristic, of not having borders and not being precisely stipulated, requires a collective and multilateral approach to ensure its governance and defense.

With this scenario, the EU has been noted as a supranational entity that aims on regulating the response to cyber attacks, through a robust legal and regulatory framework. Amongst the analyzed frameworks, the Budapest Convention is highlighted as one of the main international treaties for cooperation and combating cybercrimes, while the Tallinn Manual presents guidelines on how to apply international law on cyberconflicts, and the NIS Directive that allowed for quicker and efficient responses to attacks suffered. This analysis also shows NATO´s answer and its role in integrating cybersecurity as part of its collective defense agenda.

However, after analyzing the efficacy of said frameworks, it has been observed that although significant improvements have been made, there are still many issues to be faced. The constant technological evolution and dissemination of new actors within cyberspace, from hackers to State-Nations with vast resources, request for a constant update on norms and the creation of new strategies to deal with emerging threats. Furthermore, the coordination between different jurisdictions and harmonizing national legislations continues to be an obstacle to a truly efficient and global solution.

It is, therefore, concluded that, the existing frameworks offer an important base to safety in cyberspace, but its efficacy depends on States and international organization´s capacity to fastly adapt to changes in the cybernetic scenario. The EU, through its policies and agreements, has a pivotal role but faces challenges to reconcile its norms with other global powers, and guaranteeing the cooperation between its Member-States and international partners.

REFERENCES

ADWAITH, P. B. *Neoliberal institutionalism: towards conflict or cooperation?.* 2022. Available at: https://www.irjweb.com/viewarticle.php?aid=Neoliberal-Institutionalism-Towards-Conflict-or-Cooperation . Accessed on: 17 aug. 2024.

AKANDE, Dapo. Cyber Operations and the Use of Force. (ed.) the *Oxford handbook of cyber security*. Oxford: Oxford University Press, 2021. Available at: https://www.law.ox.ac.uk/people/dapo-akande . Accessed on: 06 sept. 2024.

AKANDE, Dapo; COCO, Antonio; DIAS, Talita, Drawing the Cyber Baseline: *The Applicability of Existing International Law to the Governance of Information and Communication Technologies.* International Law Studies, Vol. 99, 2022 . Available at file:///C:/Users/zitta/Downloads/Drawing%20the%20Cyber%20Baseline%20-%20Governance%20of%20Information%20Akande%20-%20Coco%20-%20Talita%20Dias.pdf. Accessed on 16 Aug 2024.

AJAYI, E. *The Impact of Cybercrimes on Global Trade and Commerce*. [*S. l.*], ARASI, 2016. Available at: CEEOL -

https://www.researchgate.net/publication/312658622_The_Impact_of_Cybercrimes_on_Global_Trade_and_Commerce . Accessed on: 09 sept. 2024.

ALKHADRA, Rahaf *et al*. Solar winds hack: In-depth analysis and countermeasures. *In*. *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. [*S. l.*]: IEEE, 2021. p. 1–7. Available at: https://ieeexplore.ieee.org/abstract/document/9579611. Accessed on: 29 jun. 2023.

BARKER, Ken. Cyberattack: What Goes Around, Comes Around: *Risks of a Cyberattack Strategy*. *Revista,* v., n., p., data. Available at: https://web.p.ebscohost.com/ehost/detail/detail?vid=0&sid=444aee65-4b39-400e-97fb-10984fecb86e%40redis&bdata=Jmxhbmc9cHQtYnImc2l0ZT1laG9zdC1saXZl#AN=137096668&db=aph. Accessed on: 21 aug. 2023.

BOLTON, John R. Defense threats in cyberspace. *National Review*, jul. 2021. Available at: https://www.nationalreview.com/magazine/2021/08/16/defense-threats-in-cyberspace/.Accessed on: 17 oct. 2023.

BRZOSTEK, Agnieszka. The Duties and Legal Status of the Government Plenipotentiary for Cybersecurity and the College for Cybersecurity. *Cybersecurity in Poland*: Legal Aspects, p. 277–289, 2022. Available at: https://library.oapen.org/bitstream/handle/20.500.12657/51461/1/9783030785512.pdf#page=278 . Accessed on:11 mar. 2024.

COUNCIL OF THE EUROPEAN UNION. EU-NATO Joint Declaration - 10 January 2023. Brussels: Council of the European Union, 2023. Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/. Accessed on: 30 Sept. 2024.

COCO, Antonio; DIAS, Talita. Analysis of the SolarWinds Cyberattack. European Journal of International Law, v. 33, n. 4, p. 1275–1286, 2022. Available at: https://academic.oup.com/ejil/article/33/4/1275/6881099. Accessed on: 5 Jul. 2024.

DIMITRA, Markopoulou, et. al., [*S. l.*], Volume 35, Issue 6, 2019, Available at https://doi.org/10.1016/j.clsr.2019.06.007. Accessed on 21 Oct 2024

ENISA. Threat Landscape Report. 2023. Available at: https://cyber.gouv.fr/en/french-ciip-framework. Accessed on: September 30, 2024.

ENISA. GDPR Compliance and the State of Data Breach Reporting. 2023.Available at https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing Accessed on 20 Aug 2024

EUROPEAN COMISSION, Directorate-General for Communication. (2014). *Digital agenda for Europe : rebooting Europe's economy*. Publications Office. https://data.europa.eu/doi/10.2775/41229

EUROPEAN COMMISSION. *Press release*: Die Europäische Kommission. 2022. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_2985/IP_22_2985_EN.pdf. Accessed on: September 30, 2024.

EUROPEAN COMMISSION. The NIS Directive and Its Impact on Cybersecurity. 2022. Available at https://www.nis-2-directive.com/ . Accessed on 24 Aug 2024

EUROPEAN COMMISSION. Digital Agenda for Europe: Rebooting Europe’s economy. Luxembourg: Publications Office of the European Union, 2014. Available at: https://data.europa.eu/doi/10.2775/41229. Accessed on: 21 Oct. 2024.

EUROPEAN COMMISSION. Die Europäische Kommission [Press release]. Brussels: European Commission, 2022. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_2985/IP_22_2985_EN.pdf. Accessed on: 30 Sept. 2024.

ENISA. GDPR Compliance and the State of Data Breach Reporting. European Union Agency for Cybersecurity, 2023. Available at: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing. Accessed on: 20 Aug. 2024.

FARRELL, Henry; NEWMAN, Abraham L. Weaponized Interdependence: *How Global Economic Networks Shape State Coercion*. *International Security*, v. 44, n. 1, p. 42–79, 2019. DOI: https://doi.org/10.1162/isec_a_00351. Available at: https://doi.org/10.1162/isec_a_00351. Accessed on: 22 jun. 2024.

FILHO, Oscar; A South American Defence Structure: *Problems and Prospects,* PUCRJ, Vol. 39, Ed. 03. p. 673-689, 2017. Available at: https://www.scielo.br/j/cint/a/wsvwNg84S5YWtV5JQmSK58H/?lang=en . Accessed on: 12 Oct 2024.

FREEDMAN, D. H. A Pandemic of Cyberattacks. *Newsweek Global*, [*S. l.*], v. 180, n. 3, p. 16–25, 2023. Available at: https://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=161356844&lang=pt-br&site=ehost-live. Accessed on: 18 aug. 2023.

HU, Guanhua; LI, Bing; XIU, Yuanyuan. Impact of Cyber Attacks on Trade Between Coastal Countries: An Empirical Study. *Journal of Coastal Research*, [s. l.], v. 94, p. 976–982, 2019. DOI: 10.2112/SI94-192.1. Available at: https://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=138599451&lang=pt-br&site=ehost-live. Accessed on: 21 aug. 2023.

KESSLER, Oliver; Werner, Wouter. Expertise, Uncertainty, and International Law: *A Study of the Tallinn Manual on Cyberwarfare*. Leiden Journal of International Law. 26., 2013.Available at DOI 10.1017/S0922156513000411. Accessed on 21 Oct 2024.

KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Chris. The EU General Data Protection Regulation (GDPR): A Commentary. New York: Oxford University Press, 2020. Available at: https://doi.org/10.1093/oso/9780198826491.001.0001. Accessed on: 26 Sept. 2024.

LIU, Xiang *et al*. Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, [*S. l.*], v. 13, p. 927398, 2022. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC9629147/ . Accessed on: 24 Nov. 2023.

MARKOPOULOU, Dimitra; et al. Understanding Cybersecurity Compliance: Analyzing GDPR Impacts. Computer Law & Security Review, v. 35, n. 6, 2019. Available at: https://doi.org/10.1016/j.clsr.2019.06.007. Accessed on: 21 Oct. 2024.

MCGUIRE, Michael. The Growing Threat of Cybercrime. *Journal of Cyber Policy*, [*S. l.*], v. 6, n. 1, p. 67–85, 2021. Available at: https://link.springer.com/chapter/10.1057/978-1-137-57228-8_10. Accessed on: 13 may 2024.

MOYNIHAN, H. The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy*, [*S. l.*], v. 6, n. 3, p. 394–410, 2020. DOI 10.1080/23738871.2020.1832550. Available at: https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1832550 . Accessed on: 07 Sept. 2024.

NATO CCDCOE. The Montenegro Cyberattack: Lessons in Cyber Diplomacy and NATO's Collective Defense. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2022. Available at: https://ccdcoe.org/. Accessed on: 29 Sept. 2024.

NYE, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.Available at https://www.jstor.org/stable/41149419 Accessed on: 11 Sept. 2024

PETERS, Benjamin. Rise of the Machines: A Cybernetic History by Thomas Rid. *Technology and Culture*, v. 59, p. 492–494, 2018. DOI: 10.1353/tech.2018.0049. Available at: https://doi.org/10.1353/tech.2018.0049. Accessed on: 06 Apr. 2024.

RID, Thomas; BUCHANAN, Ben. Attributing Cyber Attacks. *Journal of Strategic Studies*, v. 38, n. 1-2, p. 4–37, 2015. DOI: 10.1080/01402390.2014.977382. Available at: http://dx.doi.org/10.1080/01402390.2014.977382. Accessed on: 12 Aug. 2024.

ROATEN, M. Cyber Protection. *National Defense*, [S. l.], v. 107, n. 829, p. 22–23, 2022. Available at: https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=160390767&lang=pt-br&site=ehost-live. Accessed on: 17 Aug. 2023.

SENG, N. Cybersecurity incident reporting laws in the Asia Pacific. *International Cybersecurity Law Review*, [S. l.], v. 4, p. 325–346, 2023. DOI: 10.1365/s43439-023-00088-9. Available at: https://doi.org/10.1365/s43439-023-00088-9. Accessed on: 31 Aug. 2024.

SANGER, David E. *North Korea's Role in WannaCry and the Future of Cyber Conflict*. New York: The New York Times, 2017. Available at https://www.nytimes.com/2017/10/21/opinion/sunday/north-korea-cyberthreat.html Accessed on 13 Marc 2024.

UNDIR, A Compendium of Good Practices, *Developing a National Position on the Interpretation of International Law and State Use of ICT*, Geneva, Available at https://unidir.org/publication/a-compendium-of-good-practices-developing-a-national-position-on-the-interpretation-of-international-law-and-state-use-of-ict/ . Accessed on
Set 2024.