UNIVERSIDADE CATÓLICA PORTUGUESA

NATO and EU Cooperation on Cyber Defence

Context of the Russia-Ukraine Aggression

Eduardo Filipe Martins Fonseca Gonçalves Nunes

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024

Esta página foi deixada de forma propositada em branco.

UNIVERSIDADE CATÓLICA PORTUGUESA

NATO and EU Cooperation on Cyber Defence

Context of the Russia-Ukraine Aggression

Eduardo Filipe Martins Fonseca Gonçalves Nunes

Orientador: Prof. Dra. Maria Isabel Tavares

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024

Dedicatória

À minha família, amigos e professores,

Pelos valores e conhecimento transmitidos.

“Cooperation and determination are the two answers to the question of ending the war and bringing peace closer”, President Volodymyr Zelenskyy in a traditional address to the Ukrainian nation on February 26.

Resumo

Não é uma dimensão inovadora no espaço geopolítico, mas seguramente tem ganho importância nas posições estratégicas mundiais, no que concerne ao território ciber. Ainda que alguns países possam não ter plano e respostas para os problemas que este traz, registaram-se alguns progressos ao longo dos anos relativamente à reação coletiva das instituições internacionais.

O que os últimos anos revelaram aos estudiosos e investigadores da ciber defesa foi que o direito internacional carece de regulações específicas para governar o ciberespaço. Há alguns anos a questão era se o direito internacional se aplicava ao ciberespaço, atualmente é como se poderá adaptar o direito internacional às operações ciber.

Esta dissertação tem como objetivo discutir como a cooperação é o motor para proteger o ciberespaço, e torná-lo mais democrático. O objetivo é também entender o que as organizações internacionais têm feito para aproximar o direito internacional desse compromisso. A análise será feita nos próximos capítulos a respeito de algumas teorias e princípios.

PALAVRAS-CHAVE: Ciberespaço, Operações ciber, Cooperação.

Abstract

It´s not an innovative dimension on the geopolitical space, but surely it is rapidly winning importance in terms of the world's strategic positions, when we talk about the cyber territory. Although some countries might not have yet the plan and responses for the legal problems that it embraces, that have been some progress across the years in terms of a collective reaction from the international institutions.

What the past years reveal to the people that study and investigate cyber defence policies is that international law lacks specific regulations to govern cyberspace. Some years ago, the question was whether if international law was applied to the cyberspace, now the question is how can international law adapt to cyber operations.

This dissertation has the goal to discuss how cooperation is the engine to protect the cyberspace, and to make it more democratic. The goal is also to understand what international organizations have been doing to approach international law to this commitment. The analysis will be done in the next chapters regarding some theories and principles.

KEYWORDS: Cyberspace, Cyber operations, Cooperation.

Index

Acronyms and abbreviations

Art.- Article

ACO- Allied Command Operations

ACT- Allied Command Transformation

CFSP- Common Foreign and Security Policy

CSDP- Common Security and Defence Policy

EDA- European Defence Agency

EDF- European Defence Fund

EEAS- European External Action Service

e.g.- for example

EPF- European Peace Facility

EU- European Union

EUMC- European Union Military Committee

GDP- Gross Domestic Product

ICC- International Criminal Court

ICJ-International Court of Justice

i.e.- *id est,* this is

ILC- International Law Commission

IO- International Organization

NAC- North Atlantic Council

NATO- North Atlantic Treaty Organization

ORION- Large-scale Operation for Resilient, Interoperable, high-intensity combat-Oriented and Innovative armed forces

PESCO- Permanent Structured Cooperation

SACEUR- Supreme Allied Commander Europe

SHAPE- Supreme Headquarters Allied Powers Europe

TEU- Treaty on European Union

TFEU- Treaty on the Functioning of the European Union

UN- United Nations

U.S.- United States

Chapter I- Introduction

The actual morphology of the military operations it´s not a concept circumscribed to the traditional one. Military operations, in the common sense, refer to the air, sea and ground, and still have a big impact on the defence policy of the countries. But derived from the type of conflicts, international crisis and disputes of power in the present, it unleashed the need for the Armed Forces to include the cyberspace in its operations. Countries have been pointing cyber defence as a crucial point of their national defence programs. Portugal, since 2013 has been developing the National Cyber Defence Strategy [1]to strengthen the knowledge in this area between civilians and the Armed Forces.

Regarding the international law that applies to cyber activities, specialists in the field have voiced their opinions in two Tallinn Manuals. Furthermore, the International Court of Justice's case law and advisory opinions have been helpful in setting precedents for future discussions on the subject. International law emerges as the safest option to counter all the threats in this field of action. It allows a cooperation between non-state actors and the State´s defence department regarding the protection of the public part of the cyberspace.

Cyberspace and the Internet are being used more often by state and non-state actors for money laundering, extortion, fraud, disruption, data theft, and manipulation. The term "cyber diplomacy" refers to the use of diplomatic strategies and negotiations to address and regulate issues related to cyberspace in the realm of international relations[2]. States boost interactions between global actors in the public and private sectors by using shared and agreed rules, protocols, and behaviours.

The examination of cyberspace regulation in Western nations, including Israel, draws upon the regulatory frameworks of the United States, Britain, France, Germany, and the European Union, as well as other regulated fields like nuclear energy and environmental protection. The UN Group of Governmental Experts and the UN Open-ended Commission on the Application of Existing International Law, including the UN Charter,

[1] Estratégia Nacional de Segurança do Ciberespaço 2019-2023, (Centro Nacional de Cibersegurança de Portugal, Relatório de avaliação da execução, março 2020) https://www.cncs.gov.pt/docs/relatorioavaliacaoexecucao2019-ago2020.pdf.

[2] RADANLIEV, Petar "Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing" (2024), Journal of Cyber Security Technology.

to Cyberspace have confirmed Collaborative Unit. The United Nations General Assembly has accepted the reports from both panels[3]. Thus, two UN members have categorically reiterated that international law is applicable in cyberspace.

[3] Government Offices of Sweden, "Position Paper on the Application of International Law in Cyberspace", (July 2022), pp.1-4.

Chapter II- Theory of International Organizations

Since the ancient empires, like the Greek and the Roman, cooperation between civilizations was fortified by bilateral relationships. The concept of public international organizations has been shaped more recently, somewhere near the nineteenth century. When the concept of diplomacy and social consensus was developed, States by themselves were not capable to solve even more detailed problems. This situation feed the need to join States in public discussion forums, with shared ambitions, where they were represented to invoke their sovereign questions.

The first draft of this embryonic idea was the Peace of Westphalia of 1648, with some results for the next years, that lead to a first settlement in 1815 through the Congress of Vienna and the Treaty of Versailles in 1919.

The Treaty of Versailles [4]was truly a stepstone in this regard, as it meant the foundation of the League of Nations. After a fragile period concerning the global order, with the first World War, this project wanted to include every country that was open to dialogue, in a political organization.

Subsequently, the public inter-governmental or inter-state organization has gained significant traction in the field of international relations, leading to the creation of the United Nations and its affiliated organizations. [5]The nineteenth century has been described as "the era of preparation for international organization". The influence of global organizations surpassed the previous experiences, where it was just related to the international relations per se. international organizations in today's reality are the characterization of a soft power in terms of diplomacy, representing a new form of multilateralism, with the example of the UN providing forums for negotiations that are open to all States.

2.1- International Organizations

[4] "Treaty of Versailles: Primary Documents in American History", Library of Congress research guides, https://guides.loc.gov/treaty-of-versailles, consult. 23/ Jan/ 2024.
[5] COGAN, Jacob Katz; Ian HURD and Ian JOHNSTONE, 2016, "The Oxford Handbook of International Organizations", *1st Oxford* University Press, pp. 115-118.

International organizations comprehend three distinct modes of realization. The objective sense, that is related to the mode of structuration of the global International Community, as well as the shaping system of international relations in general. Then the subjective sense, where the international organizations are built to represent those entities by a multinational act of will and to accomplish interests from an international perspective. Finally, we have the narrower subjective sense, where this expression is utilized to represent the reality of those entities, that are subjects of international law, that have international personality, public nature, non-profit purpose and permanent and autonomous character. This last concept is the fundamental one to interpret the Law of International Organizations.

Some characteristics of International Organizations can define them as: Public collective persons of an associative nature; they act in their name but represent the interests of other subjects of International Law that are their members; they are created by the "devolution of powers", *i.e.* by an act (e.g. international treaty) which gives back powers; proceed specific public interest purposes.

These international institutions are connected to the Law of International Organizations, which is the part of objective law, that represents the system of legal norms that control the procedure of IO's. The individuals of International Law gather in an associative basis the elements needed for development and critical thinking, according to the shared interests of its own members[6].

The legislation controlling public international organizations' overall activities and organizational structure was described in 1962 by Jenks[7] who used the language of private international law as the "personal" law of the organization[8].

There are several different aspects of public international organization law that can be looked at when studying it. The "institutional" features of their operations are of relevance here.

These covers subjects as the interpretation of texts, membership, budgeting, international personality and capacities, among others. The law applicable to international

[6] Cf. D´Oliveira Martins, Margarida Salema e Afonso, 1996, *"*Direito das Organizações Internacionais", Vol. I, 2ª ed, Lisboa: AAFDL p.9.
[7] JENKS, Clarence Wilfred, 1962, "The Proper Law of International Organizations"*, Vol.2, California University.*
[8] AMERASINGHE, C.F.,2005, *"*Principles of Institutional Organizations",2nd ed, Cambridge studies in international and comparative Law, p.12-14.

organizations is further impacted by the additional functional components of organizational law. These include, the manner the UN exercises its powers of dispute settlement under Chapter VI of the Charter or peacekeeping by implementing enforcement measures under Chapter VII. However, as has been noted, it is challenging to draw a precise line separating the institutional law of international organizations from other legal disciplines that are closely related, such as the functional aspects of organizational law.

There are "laws" of international organizations, although certain authors have continuously maintained that there is no "law" of international organizations. It follows that since each organization's constitution is an independent document that contains the law governing it, neither generic law nor general legal principles that apply to all or some organizations may exist.

The way the law has developed indicates that, for certain purposes and in some regions, common legal concepts are in fact relevant, even though each organization is generally unique in terms of its institutional processes and the laws that apply to it. For example, uniformity can be seen in the broad principles that are applied, in customary international law that is applied through the application of general legal principles, and in constitutional documents due to their similarities. [9]Specifically, since a large portion of the institutional law that applies to organizations is based on how their constitutions are interpreted, general principles of text interpretation including those derived from the interpretation of other texts become applicable.

This organizational law divides into:

> *(i) constitutional texts and law-creating practices of any organization that will establish law for that particular organization (e.g. amendment and structure of organs); (ii) This similarity between constitutional texts may constitute guidelines for another organization (e.g. membership); (iii) customary international law; (iv) general principles of law (e.g. doctrine of ultra vires); (v) When implementing and interpreting organizational constitutional law, a few underlying assumptions and implicit rules will be applied as general law (e.g. international personality, liability vis-à-vis third parties of members of an organization for its obligations).*[10]

[9] KLABBERS, Jan, 2015, "An Introduction to International Organizations Law", *3rd ed,* Cambridge University Press*, pp. 2-6.*

[10]AMERASINGHE, C.F.,2005, *"*Principles of Institutional Organizations",2nd ed, Cambridge studies in international and comparative Law, pp. 16-21.

It stands to reason that judicial organs' case decisions will frequently contain principles. Therefore, there would be a focus on jurisprudence in some sections. It is often unreasonable to critique internal decisions of an organization from an external standpoint, as outsiders typically lack insight into the decision-making process. In relation to organizational practices, access to the legal opinions provided by the institutions' legal advisors would be highly beneficial. Concerns arise when organizations maintain such a level of opacity that it materially impedes access to them.

2.2- Legal Personality of International Organizations

Legal subjects in any circumstances doesn´t need to share identical rights in their nature, only depending on the necessities of their communities. We shouldn´t mistake International Organizations with the States, neither their rights and duties are the same as the States. Although IO´s are subjects of international law capable of possessing international rights and duties.[11]

Actually, it is also considered when States create International Organizations, that there is a transfer powers and attributions, and they generate feasible conditions for their own will, with the intention of giving them a legal personality. For purposes of legal security, in the founding act of International Organizations it´s included an attribution clause of legal personality.

In the case of global organizations, regarding the position of the International Court of Justice in the case Reparation for Injuries Suffered in the Service of the United Nations, [12]in conformity with international law, the majority of the States has the faculty to create an entity that possesses an objective international personality, not only recognizable by those countries.

It is noteworthy that the Court held that the ability to establish an organization with objective international personality belonged to fifty States, which together represent the great majority of the world's nations. It did not state that an entity's international personality had to constantly be created by the large majority of States in order for it to

[11] Cf. Advisory Opinion stated by the ICJ in the case Reparation for Injuries Suffered in the Service of the United Nations (in International Court of Justice, Reports and Advisory opinions, 1949, p.174 ss).
[12] Cf. International Court of Justice, Reports and Advisory Opinions, 1949.p. 185.

be successful and objective toward third States. Had it meant what it did not state, it would have meant that most international organizations that are not universal or nearly universal would not have their objective legal personality recognized.

There is doubt about the significance of an international organization's legal personality existing in national law to the development of that organization's personality in international law. The ICJ in this Reparation Case, when discussing the establishment of international personality for the UN, stated that: "It has defined the position of the Members in relation to the Organization (…) by giving the Organization legal capacity (…) in the territory of each of its members."[13]

It is important to understand where the foundation of legal personality of International Organizations comes from. There are two theories that can validate that, the objective and the subjective one. In the case of the objective theory, it´s defended that the international personality combines in a norm of international law. For FINN SEYERSTED, who defends this theory, the international organs, unless they are submitted to the jurisdiction of any country, or if they don´t assume obligations in the name of other member states, they represent the elements needed, by international law, to constitute an International Organization. In the subjective theory, it is argued that the legal personality of international organizations originates from the will of the legal subjects who establish them, giving them the authority to act in compliance with international law that was once theirs.

The prevalent perspective, upheld by IGNAZ SEIDL-HOHENVELDERN, held that international organizations were "estab-lished by the will of their founder States, merely derived subjects of public international law", and only granted the express or implied powers specified in their constituent instruments. Apart from the third states would have to decide whether to "recognize" the legal personality of international organizations or to ignore them, according to the UN (and maybe comparable bodies).[14]

Reparation for Injuries is cited in the 2011 Articles on the Responsibility of International Organizations for Internationally Wrongful Acts (ARIO) Commentaries as:

[13] Cf. International Court of Justice, Reports and Advisory Opinions, 1949.p. 179.
[14] BORDIN, Fernando Lusa, 2023, "The Quest for International Legal Status: On Finn Seyersted and the Challenges of Theorizing International Organizations Law", European Journal of International Law, Volume 34, Issue 1, pp.5.

Looking to favour the believe that an organization's legal personality is an objective personality when it exists and affirm that it is not "necessary to inquire whether the legal personality of an organization has been recognized by an injured State before considering whether the organization may be held internationally responsible.[15]

Pre-Trial Chamber I was requested by the prosecution to rule on whether the International Criminal Court may be involved in the alleged deportation of Rohingya people from Myanmar, a country that has neither ratified or signed the Rome Statute. Addressing Myanmar's stance that "no treaty can be imposed on a country that has not ratified it".[16]

The ICC's existence is an objective truth, the Chamber remarked, evoking the spirit of Special Rapporteur Gaja at the ILC, since it is a legal-judicial-institutional organization that has interacted and cooperated not just with States Parties, but with many States, whether or not they are signatories, not being Parties to the Statute.[17]

As analysed before the capacity of International Organizations to have legal personality related with the fact that they can, in the proceeding of their activities cause losses to other legal subjects, according with the principle of responsibility. This principle states that global organizations are obliged to repair the losses caused to the other subjects of law.

The facts that express a behaviour from the organs of an IO are imputable to them, and these are understandable as autonomous and institutionalized centres of power, and perceived by the national law of that organization, they can declare the will of that organization. This also can derive from the actuation of an agent that represents the institution. This responsibility most times derives from the fact that the organs of the IO can exceed their competences. The fact that generates responsibility, in this regard, can be developed in a territory subject to a jurisdiction of another subject of law. [18]

---

[15] ILC, "Articles on the Responsibility of International Organizations for Internationally Wrongful Acts" (ARIO), 2(2) ILC Yearbook (2011) 40, at 50.

[16] BORDIN, Fernando Lusa, 2023, "The Quest for International Legal Status: On Finn Seyersted and the Challenges of Theorizing International Organizations Law", European Journal of International Law, Volume 34, Issue 1, p.9.

[17] However, the chamber's reasoning highlights the conceptual ambiguity in this area, citing the Rome Statute's references to multilateral treaties and customary laws as well as the "purposes and considerations of an erga omnes character." (para. 75).

[18] See article 13º of the project of articles about State responsibility, approved in the first reading by the Commission of International Law, sessions 25º to 32º, Responsibility of States for Internationally Wrongful Acts (2001) (un.org).

Although everything that was mentioned above refers to the international responsibility of IO´s, this is just not strictly about internationally illicit facts that are imputed to International Organizations. There is just the need of verifying losses that are a result of actions imposed to the IO, even though there is no illicitness or fault that can be blamed, and automatically these actions, that create damages, must be repaired.[19]

2.2.1- The problematic of international legal personality

The ICJ rendered two significant preliminary rulings in the Reparation Case concerning the implications of international personhood for international organizations.

There can be no doubt that the Court was of the view that acknowledging that an international organization has international personality does not mean recognizing a) that it is a bigger State; b) that it is a State; and c) that it has the same rights, duties and capacities as a State. These negative claims were predicated on the ideas that legal persons are not the same under the international legal system, that their legal nature is contingent upon the demands of the international community, and that they differ "in the extent of their rights."

Having said that, a number of significant concerns emerge from the opinions of the Court as well as from the advanced ideas. Such as:

> *(i) whether inherent rights, duties, capacities proceed from the international personality of international organizations and what, if any, these are; or (ii) whether they have only powers implied in their constitutions or the circumstances of their creation; (iii) what principles, rights, duties and capacities might be implied; and (iv) what is the effect of express or implicit prohibitions in the constitutional mechanisms.*

The subject of the legal impact of personality for international organizations cannot be answered categorically, as evidenced by the ICJ's actions and statements. Although the problems are complex, it is helpful to start by reviewing the specific rulings and actions made by the Court in the cases where the matter was raised. These decisions include the

[19] Cf. D´Oliveira Martins, Margarida Salema e Afonso, 1996, "Direito das Organizações Internacionais", Vol. I, 2ª ed, Lisboa: AAFDL, p.306-316.

Reparation Case, the Effect of Awards Case[20], the Expenses Case[21], and a separate conclusion in the World Health Organization Agreement case. [22]

Therefore, the Court adopted the stance that international organizations were inferior entities while States were supreme international individuals possessing the widest range of abilities and functions. This factor might also lend greater weight to the Court's emphasis on the implied powers rather than the concept of inherent capacity.

2.3- Powers of International Organizations

This recent clarification is crucial in addressing the question of whether power is attributed or inherent. An organization may possess power by attribution, which poses no issue in its recognition. However, complexities in the analysis of powers arise particularly when these powers are implied rather than explicitly granted.

From a broad perspective, it is entirely rational to compare global organizations to a singular legal entity within a conventional legal system, acknowledging that IOs possess general powers, rights, and obligations. Logically, it is more coherent to presume that international organizations hold implied powers as conferred by their constitutions, rather than those powers being strictly defined by what their founding documents explicitly or implicitly demand or by capacities unrelated to their primary functions. [23]

The extent of powers, rights and duties, in any circumstances, will be supervised by the expressed provisions in the constitutions or by implication referring to principles, that are brought from other parts of the constitution, and that are fundamental to this implication of capacities.[24]

As it was mentioned before the Reparation jurisprudence was the place where the ICJ stated the treaty making powers of the UN. The constitutive element is always the basis to these powers for the organizations, although they have not a condition to be absolutely conferred. The only condition is to an existing correlation between the implication of

[20] 1954 ICJ Reports p.47.
[21] 1962 ICJ Reports p.151.
[22] 1980 ICJ Reports p.73.
[23] COGAN, Jacob Katz; Ian HURD and Ian JOHNSTONE, 2016, *The Oxford Handbook of International Organizations, 1st ed, Oxford* University Press, pp. 147-149.
[24] AMERASINGHE, C.F.,2005, "Principles of Institutional Organizations",2nd ed, Cambridge studies in international and comparative Law, pp. 100-101.

powers and a strong sense of inference that those kinds of powers are extremely necessary for the proceedings of the organization and the fulfilment of its requirements. For example, in the case of the United Nations, the capacity of entry treaties it´s given by his essential element. And if we look to other institutions, like the EU, it´s its constitution that allows the organization to join treaties. The principle for organizations is that the power to integrate treaties is not unlimited, even though there are no specific prohibitions to it. The capacity to make treaties is determined by an explicit strong power or by an implied power from the essential element.

In the EU legislation, there is the example of the quasi-legislative power of the EU, which is an explicit power given by its constitution. This is a specific power that brings security when applied. The case of the Security Council of the UN, within the Chapter VII of the Charter, regarding the conduction of military operations requests a different application. The power of the UN to the use of force or to conduct military operations requires a general power. According to the ICJ in the Expenses and Wall Advisory Opinions, it´s not an "exclusive competence" of the UN, transferred to the Security Council, to maintain international peace and safety. [25]

Taking the example of the EU, we see some different patterns comparing with other organizations. Among the EU powers there´s no explicit power to create customary international law. The competences of the EU are a result of the transfer of capacities from the Member States, to it to act in these areas where the Member States agreed not to interfere. [26]

International organizations may also have the implicit authority to contribute to customary international law. It is widely acknowledged and uncontroversial that international bodies possess capabilities beyond these are specifically outlined in their charters, as well as some inferred authorities. Particularly, as the ICJ stated it in Reparation for Injuries, that they have "those powers which (...) are conferred upon by necessary implication as being essential to the performance of duties".[27]

[25] Note that UN Charter, Article 24 refers to Security Council's primary, not exclusive, responsibility for the maintenance of international peace and security.
[26] KLABBERS, Jan, 2015, "An Introduction to International Organizations Law", 3rd ed, Cambridge University Press, *pp. 68-69.*
[27] DAUGIRDAS, Kristina, 2020, "International Organizations and the Creation of Customary International Law", The European Journal of International Law Vol. 31 no. 1, p.7.

When determining which powers are granted "by necessary implication", the ICJ has adopted a rather moderate stance. The ICJ independently examined if the United Nations is permitted to seek international claims for damages under two distinct categories: damages for harm to the organization and damages for injuries to specific victims. The Court reached the unanimous decision that the UN could pursue compensation for the first group. This is a more detailed explanation of how the Court did not come to this result using implied powers. The Court examined the second class with respect to implicit powers. Using the aforementioned test, the majority of the Court found that when an agent is harmed due to a breach of international law, the UN has the right to pursue international claims on their behalf and, consequently, the UN's independence. They saw this ability as crucial to preserving the independence of the UN.

Chapter III- Enforcing Cooperation: Legal Mechanisms in NATO and EU

3.1- First overview of NATO and EU

Within NATO and the EU, there are two categories of operational planning: advanced and crisis response. The first is the ongoing preparation of a potential crisis situation, and the second is the creation of a response to a specific catastrophe. Comprehensive approach is the most recent strategy developed for the institutions to solve global crises and to increase international cohesion. Thus, a significant philosophical shift in the organization's makeup is anticipated, with a focus on "collective security" as opposed to "collective defence", or striking a proper balance between the duty of self-defence (Article 5 of the North Atlantic Treaty) and safety (stabilization missions and expeditionary forces).[28]

The Treaty on European Union established the Common Foreign and Security Policy of the European Union, which aims to uphold international peace and security, advance international cooperation, and build and strengthen democracy and the rule of law. The leaders of state and government of the EU member states make up the European Council, which has the last say on matters of foreign policy.

The European Union Military Committee appears as the platform of discussion between the member states in terms of objectives for the defence of the European territory. The heads of defence of the member states, who are usually represented by their permanent military envoys, make up the EUMC. All military operations inside the EU framework are overseen by the EUMC, which also plans and executes military missions and operations in accordance with the Common Security and Defence Policy and develops military capabilities. It provides the Political and Security Committee with military advice and recommendations.

When used in reference to Europe, the phrase "protection" has occasionally been confused with the term "defence". Discerning the differences between these two terms, the ensuing assignments, and the first course of action has been to underline the

[28] PAIVA DA CUNHA, Agostinho, "Acerca do Conceito Estratégico da NATO. A Caminho de Lisboa, uma Nova Estratégia para o Século XX", Repositório Comum,31 de janeiro de 2010, p.124-125.

distinctions between the roles played by the EU and NATO in the security and defence of Europe[29].

In the institution NATO all forces are part of the inflexible military organization. The International Military Staff, the Military Command Structure, the Military Committee, which is made up of the Chiefs of Defence of NATO member nations, and its executive body are the main components of the alliance's military structure. Allied Command Operations and Allied Command Transformation are the two main strategic commands that make up the NATO Command Structure. [30]

The NATO-led operations, are military guided by the Supreme Allied Commander Europe. He conducts the ACO.[31]The legal office, ACO Office of Legal Affairs (ACO OLA) provides advice to all SHAPE staff branches, the Supreme Allied Commander Europe, and his Command Group. It is the last supervisor within ACO for all issues pertaining to Supreme Headquarters Allied Powers Europe's and the subordinate headquarters' obligations, functions, operations, and activities, as well as any issues that may have legal ramifications for North Atlantic Council's mission to SACEUR.

Through the work of the European Defence Agency, in conjunction with Europol and the EU cybersecurity agency, the EU collaborates on cyberspace defence. The EDA guarantees the availability of both proactive and reactive cyber-defence technology and assists member states in developing a trained military cyber-defence staff. The EU and NATO will continue to collaborate on improving shared situational awareness, strengthening cyber capabilities, and preventing, deterring, and responding to cyber threats in accordance with the EU Strategic Compass and the EU Policy on Cyber Defence.

3.2-EU and NATO functional methodology in security and defence

According to some observers, two decades of comparatively stable global conditions have progressively given way to chaos and anxiety, making global instability "the new

[29] KOSTAKAROS, Mikhail, “Guest Editorial”, European Foreign Affairs Review 23, no. 4 (2018), pp. 436–437.
[30] In this sense, see: https://shape.nato.int/page11283634/knowing-nato/episodes/the-nato-structure.
[31] NAUTA, David, 2016, The International Responsibility of NATO and its personnel during military operations, Doctoral Thesis, Radboud University Nijmegen, pp. 65-69.

normal." Conflicts have increased since 2012, with a spike in civil wars. For the first time in ten years, the number of attacks carried out by nations and armed groups is rising. Terrorism, violent extremism, and hybrid threats are just a few of the emerging challenges that pose a serious threat to global security, peace, and stability.

The EU Council adopted the policy in November 2016, [32]with an emphasis on increasing strategic autonomy, fostering an integrated approach to conflict and crises, and fostering resilience.

The Member States of the European Union have primary authority for security and defence policy. In addition, the Lisbon Treaty establishes a shared security and defence strategy that may eventually result in a European defence union. [33]Since 2016, there have been notable advancement in that regard, with a number of security and defence-related projects having been suggested and started within the Commission and European Parliament's 2014–2019 mandate.

Thirty years after the EU's Common Foreign, Security, and Defence Policy was incorporated into the Treaty, "specific rules and procedures" continue to appear to impede the policy's efficacy. Remembering that the CFSP is mandated to "cover all areas of foreign policy and all questions relating to the Union's security" (Art. 24 TEU), as stated in the Treaty in short.

The competences of the EU in the military sphere are not explicit in the TEU.

Article 42 (7) TEU states:

> *If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States". However, the Articles are not the same. The most significant difference is that Article 42 TEU, which more broadly refers to "aid and assistance", does not specifically mention the word "military.*

The neutral and non-aligned members found it simpler to accept the commitment when the word "military" was removed. The strategy of "all the means" is thorough, but it gives

[32] Council of the EU, 14 November 2016, Council conclusions on implementing the EU Global Strategy in the area of Security and Defence. eugs-conclusions-st14149en16.pdf (europa.eu), consult. 15/ Feb/2024.
[33] RANGEL DE MESQUITA, Maria José, 2011, "A Actuação Externa da União Europeia depois do Tratado de Lisboa", Almedina, pp. 394-414.

the attacked Member State the freedom to determine what kind of support it requires and the others the freedom to outline potential forms of that support.

It is noteworthy that the selection of a Decision's legal foundation heavily influences how the Union has exercised its authority under CFSP. Additionally, the application of any legal foundation is constrained by the overarching principles and values of the EU, which are applicable to CFSP as well.[34] As such, it is the most accurate method for evaluating how the Union has applied its authority.

The Treaty of Lisbon clarifies the division of competences between the EU and its Member States. The Treaty on the Functioning of the European Union (TFEU) makes a distinction between the following categories of competence: exclusive, sharing, coordinating, supporting, and supplementing (articles 3,4 and 6). But the Union's authority over the CFSP does not fit into any of these categories; rather, it is mentioned individually in article 2(4) TFEU.

Article 2(4) TFEU states that the Union "shall have competence, in accordance with the provisions of the Treaty on European Union, to define and implement the CFSP", without going into detail about what exactly qualifies as competence to carry out the CFSP. Establish a unified foreign and security strategy, which should include a common defence strategy that is gradually framed.

Art. 2(4) refer to Art.24(1) second paragraph TUE which embodies de distinct nature of the CFSP. It refers also to Art. 40 TUE, that specifies this norm in matter of competences.[35]

In terms of CFSP, Member States are obligated to fulfil three key tasks[36]. Article 24(3) TEU outlines a general loyalty responsibility that states that "The Member States shall support the Union's external and security policy. Actively and unconditionally in an

[34] In addition to the principle of conferral (Article 5(2) TEU), which restricts the Union's authority to that which has been transferred to it by the Treaties, the other fundamental principles and values that govern the Union's operations also apply to the field of CFSP. See in WESSEL, RAMSES A. et al, "The future of EU Foreign, Security and Defence Policy: Assessing legal options for improvement", European Law Journal, Vol 26, 2021, pp.374-388.

[35] PORTO LOPES, Manuel e Gonçalo ANASTÁCIO (Coordenadores), 2012, "Tratado de Lisboa Anotado e Comentado", Almedina, p.204-207.

[36] KOUTRAKOS, Panos, "The European Union´s Common Foreign and Security Policy after the Treaty of Lisbon", Published by the Swedish Institute for European Policy Studies, Report No. 3 May 2017, pp.16-31.

attitude of allegiance and cooperation, and will abide by the Union's decision in this regard."

The EU is implementing more capable politics in terms of its external action services. The diplomatic service of the European Union is called the European External Action Service (EEAS). Implementing the EU's Common Foreign and Security Policy since 2011, the EEAS advances global peace, prosperity, security, and European interests. Part of the EU's comprehensive approach to crisis management, the CSDP draws on both military and civilian resources to allow the Union to play a leading role in peacekeeping operations, conflict prevention, and strengthening international security.

As a European mechanism for the 26 participating Member States to cooperatively build defence capabilities, coordinate investments, and improve the operational readiness, interoperability, and resilience of their armed forces, the Permanent Structured Cooperation (PESCO) is a crucial framework. It helps to put the Strategic Compass into practice and strengthens the EU's capacity to handle both present and emerging security issues.[37] It seeks to improve Member States' capacity to counter traditional threats, deliver next-generation capabilities, and offer key capabilities with a stronger operational focus. It creates connections with other defence programs and tools like the Coordinated Annual Review on Defence, the EU Capability Development Priorities, and the European Defence Fund and is essential to defence cooperation within the EU.

Moreover, the EDA is actively involved in two military mobility projects under the Permanent Structured Cooperation framework: the Netherlands-led "Military Mobility" project and Germany-led "Network of logistic hubs in Europe and support to operations". They oversee the advancement of the massive influx and movement of military people and gear. The European Union has introduced an updated "Action Plan on Military Mobility 2.0" that offers a thorough framework for creating a network of military mobility that is well-connected, has faster reaction times, and has robust, sustainable, and secure transportation infrastructure.

Regarding Russia´s war of aggression against Ukraine, in a speech on 30 January, EU High Representative, JOSEP BORRELL, stated:

> *In a conflict every second matter. Investing in military mobility is not just a commitment; it is an investment for today and tomorrow to allow our armed forces*

[37] See PESCO program in https://www.eeas.europa.eu/sites/default/files/documents/2024/2024-03-PESCO-Deepening-defence-cooperarion.pdf, consult in 06/Feb/2024.

to respond faster to crises at our borders and beyond. Efficient and seamless transportation of troops and materials across Europe is a logistical, administrative and infrastructure challenge. We must address bottlenecks through cooperation and investment, to ensure rapid movement for the security of Europe.[38]

Military mobility is frequently denoted as the cornerstone of cooperation between the EU and NATO. This endeavour encompasses amplifying the digitization of administrative protocols and orchestrating the synchronization of transnational air, maritime, and terrestrial transit. Such initiatives form the foundation of the European Continent's preparedness for defence.

In a time of geopolitical rivalry and challenges to international security, the European Peace Facility increases the EU's capacity to safeguard its partners and citizens. Since 2021, Member States have contributed to the EPF in addition to their contributions to the EU budget, acting as a single financing mechanism for the EU's military and defence operations[39]. The EU's capacity to act as a global security provider is aided by the operations pillar of the EPF, which provides collective funding for military missions and operations carried out in accordance with the Collective Security and Defence Policy, as mentioned before. This is done through the assistance measures pillar.

The Alliance's deterrent and defence posture changed significantly as a result of the Readiness Action Plan (RAP), which was introduced at the Wales Summit in 2014. The Concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA) was agreed by the Allies in 2020. In a multi-domain environment, the DDA Concept offers NATO Allies a unified, cogent framework to contest, deter, and defend against the Alliance's principal threats. The NATO 2030 agenda was agreed upon by the Allies at the Brussels Summit of 2021 in order to fortify the Alliance and direct its future adaptation[40].

3.3- Funding of NATO and EU

[38] Speech given in a "High Level Symposium" on military mobility at the Royal Higher Institute for Defence in Brussels, organised by the European Defence Agency (EDA) in the context of the Belgian Presidency of the Council of the EU. See in Military Mobility in Europe: Cooperation going in the right direction, but long road ahead (europa.eu), consult. 23/Feb/2024.

[39] The European Protection Fund (EPF) is a €12 billion fund established by the EU to aid in defence and military operations.

[40] NATO policies in https://www.nato.int/cps/en/natohq/topics_133127.htm.

Upon examining the regulations pertaining to the European Union's defence budget, it becomes evident that there has been a notable shift in stance since 2022 concerning the Ukrainian conflict. Fundamentally, the sponsorship of weaponry acquisition by the Ukrainian armed forces by the European Union constitutes a clear violation of the Union Treaties. The financing of the Union's Common Foreign and Security Strategy, inclusive of its defence strategy, is regulated by Article 41 of the EU Treaty. Consequently, the financial burden of the Common Foreign and Security Policy falls upon the Union budget, encompassing both operational and administrative expenses for concerning foreign and security policy. Nevertheless, expenditures arising from defence or military measures are explicitly excluded from eligibility for funding from the Union budget, as delineated in Article 41(2) of the TEU.

The CSFP operations are financed by an ad hoc mechanism. Financing is up to the Member States that are part of the military operations, and the some of the common costs can be funded by the Athena Mechanism.[41]

The exigency for synchronized European initiatives in defence policy affairs is underscored by the ongoing conflict in Ukraine. Undoubtedly, the Union will capitalize on the crisis to advance the integration of defence policy, particularly in the realms of territorial defence and European alliance. Although the absence of budgetary funds is not legally intended to restrict the activities of the Union's military agency, in practice, it does so. This implies that Union initiatives pertaining to military and defence policy must consistently rely on ad-hoc funding. [42]This underscores the significance of the Council's adoption of the European Peace Facility in 2021.

This concerted effort by the International Organizations is funded by plans that are decided and discussed in the heart of institutions. The EPF as an EU instrument to fund and guarantee the world´s peace and security is worth more than €17 billion funded over a seven-year period (2021–2027) outside of the EU budget. The European Union provided the Ukrainian armed forces with €11.1 billion in support between 2022 and 2024 under the European Peace Facility. The EU established the Military Assistance Mission to support Ukraine in 2022. The mission's objectives are to defend the civilian populace

[41] PORTO LOPES, Manuel e Gonçalo ANASTÁCIO (Coordenadores), 2012, "Tratado de Lisboa Anotado e Comentado", Almedina, p.156-157.
[42] VON ACHENCACH, Jelena, "Too Little Politics in EU Defence Policy- The EU Arms Supplies to Ukraine from the Perspective of Budgetary and Constitutional Law", Verfassungs blog on Matters Constitutional, March 2022.

from Russian military aggression while enhancing the fighting prowess and adaptability of the Ukrainian armed forces.

Another crucial fund for the EU affairs, and to promote the capacity of research and development of defence technologies is the European Defence Fund. Within the framework of the EDF Programme Committee, the EDA and the EEAS collaborate closely to develop the annual work plans for the EDF.

Through a cost-sharing mechanism determined according to the gross national income of each member nation, all Allies contribute to the financial resources of NATO. This exemplifies the operationalization of the common funding concept, elucidating the principles of burden-sharing within the Alliance.

NATO leaders committed to a long-term commitment to allocating at least 2% of Gross Domestic Product each year for defence when they adopted a new defence investment pledge at the Vilnius Summit in 2023. Following the identification of a particular initiative or priority, the Resource Policy and Planning Board evaluates whether the concept of common funding is applicable, i.e., whether supplying a capability or carrying out an activity serves the interests of the Alliance collectively and ought to be funded by common funding. [43]

In 2023, the Allies sustained their augmentation of defence budgets, as well as the development of forces and capabilities, and their engagement in operations, missions, and activities under the Allied framework. Notably, for the seventh consecutive year, both Canada and its European counterparts amplified their defence budgets. In real terms, defence expenditure witnessed an increase of 11% compared to the figures of 2022. Last year, in contrast to just three Allies in 2014, 11 Allies reached the standard of allocating 2% of their GDP to defence in early 2024, when that number grew to 18.[44]

During the year of 2024, not even two-thirds of the Allies reached the 2% target, which is somehow worrisome, keeping in mind all the geopolitical tensions across the globe. The discourse on burden-sharing has excessively centered on the financial allocation to defence, neglecting the shared responsibilities and adherence to agreements among the involved parties.

[43] See "The funding of NATO" in https://www.nato.int/cps/en/natohq/topics_67655.htm, consult. 28/Mar/2024.
[44] See "The Secretary General's Annual Report 2023" in https://www.nato.int/cps/en/natohq/opinions_223291.htm.

In order to deploy the requisite capabilities aimed at mitigating NATO's military risk, the subsequent course of action involves reassessing the mechanisms by which countries attain the 2 percent commitment. Important measures would be- include defence preparedness and efficacy; More transparency; Incorporate aid measures to third countries (e.g. EU countries providing material to Ukraine); Encourage countries to allocate their defence funds flexibly to repair capacity gaps in other NATO or important non-NATO countries. Leaders of NATO should also take in consideration allies spending through other institutions as the EU and investments in strategic position of the alliance.[45]

3.4- Decision-making process in the last years

Regulations from the European Union appear to have answers for every issue in Brussels. However, they become difficult outside of Brussels. States and problems are handled case-by-case in an atmosphere created by their overwhelming and growing complexity. As a result, the EU becomes weaker and eventually fragments. Nationalism increases as a result of Europeans' mistrust of the EU bureaucracy, which is run by an aristocratic, remote system.

The European Union is confronted with some significant regulatory challenges. The enormous Brussels administration has grown increasingly complex; the business community and general public find it difficult to comprehend the restrictions that Brussels faces.[46] The national governments now find it much more difficult to support the implementation of the Brussels guidelines due to the heightened resistance that has followed. Additionally, this has made the EU regulatory agencies less effective at solving issues, which has caused a regional response to certain issues.

The EU, as mentioned before, acted in a more expansive way, behind the scope of the treaties since 2022. Regardless of the outcome, the incursion of Russia into Ukraine has brought about a transformation in the security landscape of Europe. The United Kingdom is engaged in close collaboration with the European Union, while Germany has committed to rearming. Moreover, Finland and Sweden, traditionally neutral nations,

[45] MCINNIS Kathleen and Daniel FATA, "From Burden Sharing to Responsibility Sharing", Center for Strategic and International Studies (2023), p.6-9.
[46] COLIBASANU Antonia, "Decision-making and disarray in the EU", July 2016, see in https://www.euractiv.com/section/euro-finance/opinion/decision-making-and-disarray-in-the-eu/, consult in 15/Feb/ 2024.

have opted to align themselves with NATO. Nevertheless, Western nations have extended substantial military and financial support to Ukraine, concurrently imposing unparalleled economic sanctions on Russia, akin to economic warfare. [47]

The EU's inability to approve the aid package, before Viktor Orban recently lifted the veto, [48]coincides with similar challenges in the U.S. Congress. Despite the fact that treaties have remained unchanged, the EU has begun to alter its approach, driven by the necessity to achieve geopolitical independence. Consequently, the EU is taking steps to revise its treaties. Discussions on Treaty amendments should commence with the European Parliament's resolution dated November 22, 2023, which proposes 245 amendments. [49]Many of these suggested changes aim to diminish the veto powers held by individual states. [50]

While Germany has made notable strides in enhancing its individual defence capabilities, such advancements do not detract from the collective efforts of the European Union. In recent months, there have been growing apprehensions regarding the bilateral rapport between France and Germany, with Germany predominantly prioritizing its fundamental industrial defence interests. A case in point is the recent accord to procure an air and missile defence shield involving 14 NATO countries, a venture referred to as the European Sky Shield Initiative. Germany and France should work together more on developing technologies and systems, and they should prioritize supporting the creation of a more cohesive European defence industrial base.

The sustainability of Ukraine's existence has been substantially reliant on financial and material support from the United States for Kyiv and its leadership. Germany stands prominently ahead of other nations in this sphere, being the second-largest contributor in terms of both financial aid and provision of weaponry. [51]The influence exerted by the United States affects the response of the European Union, consequently influencing the stance of Germany. Hence, Secretary of Defence LLOYD J. AUSTIN III asserted that

---

[47] THOMSON, Catarina P., "Foreign policy attitudes and national alignments in times of Chinese and Russian threats: public opinion across three NATO members", The RUSI Journal 167: 2, 2022, pp. 24–37.
[48] Regulation (EU) 2024/792 of the European Parliament and of the Council of 29 February 2024 establishing the Ukraine Facility.
[49] European Parliament resolution of 22 November 2023 on proposals of the European Parliament for the amendment of the Treaties (2022/2051(INL)).
[50] DABROWSKI, Marek, "To become a geopolitical player the European Union needs Treaty change" (2024), Bruegel.
[51] See, the arms and military equipment Germany is sending to Ukraine, in: https://www.bundesregierung.de/breg-en/news/military-support-ukraine-2054992.

Ukraine remains resolute in confronting the Russian invasion of the country, and similarly, the United States stands unwavering in its support.[52]

PESCO is the lever for the industry of defence in the EU with more than 68 on-going projects. These initiatives convene Member States to facilitate the exchange of expertise in targeted sectors, engage in collective training and exercises, or cultivate novel proficiencies. In May 2023, eleven new projects were sanctioned, with objectives ranging from fortifying the safeguarding of critical seabed infrastructure to enabling specialized communication and medical support capabilities tailored to the EU Rapid Deployment Capacity.

Through their engagement in PESCO, the participating member states are enhancing their defence budgets and investments, standardizing domestic protocols, enhancing force readiness and interoperability, and collaborating in realms such as capability enhancement, training, and joint exercises. PESCO represents, in an implied way, an economic policy and aims to strengthen the autonomous defence capacity of EU member states through heightened cooperation among European Union members and synchronized efforts in capacity building.

The prevailing challenge primarily revolves around incentivizing European defence industries to augment their production output, rather than solely focusing on persuading nations to provide arms to Ukraine.

Europeans are compelled to allocate funds to replenish their depleted military supply reserves, often relying on the United States as the primary source of such resources. Despite ongoing initiatives within European defence industries, a significant portion of European defence funding is directed towards interim measures. [53]This underscores a growing dependence on the U.S. defence sector within Europe.

3.5- The EU's military development was supported by NATO and how it allowed to strengthen cooperation

[52] Secretary of Defence Lloyd J. Austin III in the 20th meeting of the Ukraine Defence Contact Group at Ramstein Air Base, Germany, see in: https://www.defense.gov/News/NewsStories/Article/Article/3711625/us-will-not-back-down-on-support-for-ukraine/ .

[53]TOCCI Nathalie, "How the war in Ukraine has transformed the EU", November 2023 https://www.socialeurope.eu/how-the-war-in-ukraine-has-transformed-the-eu.

The Helsinki Conference was one of the first drafts about peaceful cooperation and development of peace and justice in Europe. It was determined at the time in this conference, some relevant principles in terms of what we have nowadays in international law. The principle of territorial integrity of states, inviolability of borders and abstaining from resorting to the threat and use of force were declared to use in practice. The UN Charter, as one of the initial instruments, significantly influenced European thought by establishing principles such as conflict resolution through peaceful means, article 33, and advocating for general and complete disarmament.

More than 20 years have passed since the NATO and EU first cooperated. Three Joint Declarations (in 2016, 2018, and 2023), the NATO Strategic Concept, and the EU Strategic Compass (in 2022) have all been built upon.

As a follow-up, in December 2016, the Foreign Ministers of NATO endorsed 42 specific measures to advance the cooperation between the EU and NATO in seven key areas of common interest: cyber security and defence; exercises; developing defence capabilities; industry and research for defence; countering hybrid threats; and building partners' capacity for defence and security. The European Council's June 2018 call for deeper NATO-EU cooperation was also welcomed by NATO leaders, who acknowledged that the two organizations' continuing, separate strategic processes present a chance for increased dialogue and collaboration.

The third Joint Declaration seeks to deepen and broaden the strategic alliance between the EU and NATO in the wake of the adoption of the EU Strategic Compass and the 2022 NATO Strategic Concept[54]. The leaders of the two organizations decided to deal with the defence of vital infrastructure, resilience concerns, and the escalating geostrategic rivalry. The security ramifications of climate change, space exploration, emerging and disruptive technologies, and thwarting foreign meddling and media manipulation are among other high-priority areas of focus.

In view of all the EU initiatives previously mentioned they result from a strong cooperation, more efficiency and a raise of resources allocated to defence. NATO was the first partner of EU to give recommendations about the goal of the creation of a European common defence policy. According to Article 42(2) of the Treaty of Lisbon,

[54] See in NATO relations with EU in https://www.nato.int/cps/en/natohq/topics_49217.htm, consult. 06/Feb/2024.

the EU has a unified defence policy. The treaty does, however, also expressly highlight the significance of national defence policy, including neutrality or membership in NATO. In order to generate synergies at the EU level and improve protection for Europeans, the European Parliament has continuously backed greater collaboration, investment, and resource pooling.

Collaboration is essential for bridging the military viewpoints of NATO and the civilian background of the EU—two components that are essential for tackling hybridity. Furthermore, it is clear that NATO and the EU created structures that permit comparable assessments of the dangers (e.g., staff discussions, legislative inputs, joint threat assessments, and exchanges) and coordinated responses (practiced in joint exercises). However, the degree to which member states will benefit from having access to the organizations, resources, and knowledge that both parties jointly built in order to bolster and maximize their own domestic capabilities is still up to them. [55]

The type and scope of actions demonstrated the importance of institutions, and when required, they expand connections, modify already-existing structures, or establish new organizations in the fields deemed advantageous for collaboration. The window of opportunity to establish and modify the operations of both organizations was affected by external events, and these actions may be pertinently examined within the framework of discursive institutionalism.

Therefore, it is reasonable to anticipate that NATO's strength and legitimacy will continue to grow, that EU-NATO collaboration will increase, and that the EU's cohesion and ability to act internationally will be preserved and the U.S. will maintain its political and military presence in Europe.[56]

The current uncertain security environment presents new and complicated difficulties and threats that neither NATO nor the EU could handle alone, necessitating a strengthening of the cooperation. The so-called comprehensive approach to security, which frequently calls for not just military or political but also civil means—of which the EU possesses the majority—also raises the need for cooperation.

---

[55] FILIPEC Ondřej, "The cooperation between EU and NATO in response to hybrid threats – A retrospective analysis from the institutionalist perspective", Slovak Journal of Political Sciences, Volume 23, No. 1, 2023, pp.43-47.

[56] POLCIKIEWICZ, Zdzislaw, "Cooperation between NATO and the European Union for shaping international security", The Copernicus Journal of Political Studies, 2019, Pp. 75-82.

3.6- Using Strategic Autonomy as an instrument to unify Europe

There´s some geopolitical changes that possibly can happen in the near future, one of them is in the US. The presidency of Donald Trump was anything but peaceful in its relations with International Organizations. THIERRY BRETON once gave an insightful update about this situation "Back to 2020 (…) We were in Davos. And Donald Trump said to Ursula, "you need to understand that if Europe is under attack we will never come to help you and to support you, and by the way NATO is dead, and we will leave, we will quit NATO."[57]

More recently, Trump brought back the idea that the US is investing too much in support of the Atlantic countries that do not match the budgetary requirements, expansively having said he would "encourage Russia to do whatever the hell they want" to any of the US's NATO allies whom he considers to have not met their financial obligations.[58] NATO members stipulated in Article 5 of the founding treaty that any armed aggression occurring in Europe or North America "shall be deemed an attack against all ". The foundational principles of Article 5 were brought into question by Trump when he suggested that he might refrain from employing force to defend an ally.

The Council Conclusions issued in December 2013 mark a significant milestone, as European leaders advocated for measures aimed at reinforcing a European defence technical and industrial base. This initiative was intended to "enhance [the EU's] strategic autonomy and its ability to act with partners", representing the inaugural reference to Strategic Autonomy within an official EU document. [59]

In the preface of the French Defence and National Security Strategic Review of 2017, President Macron asserts that "Europe's progress on defence must be further consolidated. We have laid the foundations for its strategic autonomy." [60] According to President Macron, the essence of SA embodies a sovereigntist perspective, underscoring the capacity to act autonomously, free from dependence on external actors.

---

[57] See in, Brussels Playbook from Politico, "Kyiv seeks air defence missiles at NATO-Ukraine meeting" by Jakob Hanke Vela with Zoya Sheftalovich, https://www.politico.eu/newsletter/brussels-playbook/kyiv-seeks-air-defense-missiles-at-nato-ukraine-meeting/, consult. 15/Mar/2024.

[58] Trump´s speech in Conway, South Carolina, February 2024, https://edition.cnn.com/2024/02/10/politics/trump-russia-nato/index.html , consult. 25/ Feb/2024.

[59] European Council. (2013) Council Conclusions. 19–20 December 2013. See in: pdf (europa.eu), consult 10/ Mar/2024.

[60] Defence and National Security Strategic Review (2017) see in: https://www.dsn.gob.es/sites/dsn/files/2017%20France%20Strategic%20Review.pdf.

Looking at the signals, when the U.S. were distancing themselves from commitments with NATO, it´s safe to say it was a missed opportunity for the European countries to take over the reins of NATO. As the current situation stands, the Alliance relies predominantly on the United States for critical capabilities such as missile defence, air-to-air refuelling, operational intelligence, and various other essential components. Although, certainly it would have been a crucial situation for the European strategic autonomy.

The European Union finds itself at a pivotal juncture, where failure to navigate effectively may result in the forfeiture of its global influence. In the absence of enhanced integration, the realization of European strategic autonomy remains elusive. [61]

The conflict in Ukraine has provided a boost to the country's economy, despite the absence of direct involvement by the United States in the fighting. Defence production has witnessed growth over the past two years, with estimations by the Biden Administration indicating that approximately $61 billion in additional support from Ukraine has been directed towards U.S. defence installations.[62]

Europe may find itself in a position where it is too late to fully comprehend its circumstances, even if it were to awaken to them. In principle, Europe should possess the capability to sustain itself independently, considering its collective military expenditure is approximately three times greater than that of Russia, coupled with its significantly larger economy. The pressing concern lies in the diminishing window of opportunity for Europe to address these challenges effectively. [63]

The overwhelming majority of member states persist in their conviction that free trade and resilient multilateral institutions constitute the foundational pillars of European prosperity.[64] Additionally, they maintain that maintaining reliance on NATO represents the optimal approach to safeguarding European security. However, differing viewpoints persist within coalitions, rendering it premature to definitively assert whether a paradigm shift will transpire.

[61] GONZÁLEZ LAYA, Arancha, "La EU, entre lo inevitable y lo impossible", April 2024, Abc.es.
[62] FAIRLESS, Tom, "How War in Europe Boosts the U.S. Economy", The Wall Street Journal in https://www.wsj.com/economy/ukraine-war-europe-american-economy-654ca41b, consult, 18/ Mar/2024.
[63]GNESOTTO Nicole, "La puissance et l'Europe", Paris: Presses de Sciences Po, (1998).
[64] JUNCOS, Ana E. and Sophie,VANHOONACKER, "The Ideational Power of Strategic Autonomy in EU Security and External Economic Policies", Journal of Common Market Studies (2024), pp.1-18.

Chapter IV- Challenges of the Ukrainian war for the Cyber domain

4.1- Plans for Cyber Defence

The cyberspace is a topic that barely was discussed until some attacks occurred in 2007 and 2008 to Estonia and Georgia. That are not much practical cases to analyse, and that was the reason for the legal advisors of NATO to design a legal framework to ensure that cyber operations can be developed in peace times. At the same time States were forced to developed their own national cyber defence strategy. The stage of evolution in these national strategies is very different, what reinforces the need of international cooperation to avoid cyber threats. [65]

In actuality, NATO has said that you can act to address a specific situation without having to invoke Article 4. Nonetheless, NATO's involvement in reactions to cyberattacks that are "below the attack threshold armed" may result in further issues with international law. [66]

After 2008 in the EU that was a great sense of insecurity and vulnerability in the defence of cyber space. The Member States also "accused" of a significant deficiency: there was a severe lack of information integration and communication, which meant that different components of cybersecurity and cyber defence were implemented in different nations. Therefore, in an effort to address these shortcomings on the part of the Member States, the 2012 European Parliament Resolution Proposal calls for a cooperative plan between the EU States and the United States of America, which currently positions itself as the nation with the most advanced cybersecurity and cyber defence issues. [67]

Some of the measures of this resolution consisted in the creation in the EU of a single, comprehensive strategy plan that defines cybersecurity and cyber defence in detail; Make a distinction between the many cyberattack levels in the political and military domains based on their objectives and outcomes; The European security strategy should be

[65] TSAGOURIAS, Nicholas and Russell BUCHAN,2023, "Research Handbook on International Law and Cyberspace",*2nd ed,* Edward Elgar, pp. 224-229.
[66] TSAGOURIAS, Nicholas and Russell BUCHAN,2023, "Research Handbook on International Law and Cyberspace",*2nd ed,* Edward Elgar, pp. 521-522.
[67] See "European Parliament resolution of 22 November 2012 on Cyber Security and Defence (2012/2096(INI)": https://eur.lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52012IP0457&qid=1559117228462&from=EN, consult. 25/Mar/2024.

updated and modified, primarily in the internet part, to make it easier to identify and learn how to spot cyberattacks and track down the people who launched them. As a response to these goals the EU implemented, as a primary measure, the Community Emergency Response Team (CERT) which is an experienced group that can respond quickly in the event of a cyberattack, ideally within a day.

In the cyber domain a comprehensive Cyber Defence Policy, which serves NATO's three main missions as well as its overall deterrence and defence posture, was approved by Allies at the 2021 NATO Summit in Brussels. NATO's defensive mission was reiterated by the allies, who also pledged to use all available means to actively prevent, defend against, and neutralize all cyberthreats, including by taking coordinated action. [68]

European Union Commissioner for Internal Market THIERRY BRETON declared in 2021 that the EU lacked a cyberspace doctrine. [69]The European Union's cyber defence strategy is based in a current defensive approach of trying to dissuade adversaries from attacking. The EU still heavily rely on the cyber defence plans of each member state. The EU can´t compete, in the cyber domain, with other powers like China, North Korea or Iran. CHARLES MICHEL, President of the European Council, recently warned for a change of strategy having envisaged:

> *It would help us to take a position of leadership in cyber response operations and information superiority, and I believe it should be equipped with offensive capabilities (...) We should identify flagship capabilities at European level (...) For instance, capabilities that are European by nature, like the strategic enablers, like cyber capabilities or satellites or strategic transportation.*[70]

4.2- The non-traditional start of the conflict

Russia's incursion into Ukraine on February 24, 2022, termed by Russia as a "special military operation", should be comprehended as a hybrid warfare strategy that

[68] NATO Cyber Defence Policy in https://www.nato.int/cps/en/natohq/topics_78170.htm,consult. 25/Feb/2024.
[69] Single Market Programme 2021-2027: closing statement by Thierry BRETON, European Commissioner for Internal Market, Single Market Programme 2021-2027: closing statement by Thierry BRETON, European Commissioner for Internal Market - Multimedia Centre (europa.eu).
[70] Annual conference of the European Defence Agency (EDA), 30 November 2023, see in https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/a-european-defence-for-our-geopolitical-union-speech-by-president-charles-michel-at-the-eda-annual-conference/,consult. 15/Mar/2024.

encountered setbacks. However, Russia's subsequent actions after the initial setback in late February 2022 necessitate examination and consideration within the framework of conventional warfare theory, rather than solely as an aspect of the "hybrid war" paradigm.

Regarding the initial inquiry, it could be contended that Russia's military aggression against Ukraine commenced in 2014 through the annexation of Crimea and its intervention in the Donbas region. The subsequent full-scale invasion may be considered a legal extension of those preceding actions. The invasion of 2022 seems to have been perceived as a completely different occurrence requiring its own justification, given that it represents a novel application of force.

The operational conduct of the Russian Armed Forces, particularly in their strategic and tactical approaches to warfare, frequently falls short of even the most fundamental international standards delineated by the Humanitarian Laws of Armed Conflict. This deficiency introduces an organizational or systemic element to the catalogue of observed war crimes perpetrated by individual soldiers. Additionally, from a moral vantage point, the adoption of the term "hybrid" as a descriptor, intended to mitigate the explicit invocation of "war," risks diminishing the gravity of the sacrifices endured and the suffering endured by the Ukrainian population.[71]

Much to the profound surprise of Western observers, they noted a departure from contemporary warfare doctrines characterized by precision-guided munitions aimed at minimizing civilian casualties.

Even in anticipation of Russia's invasion on February 24th, Ukraine lacked practical means to pre-emptively deter such a significant strike. Moreover, initiating hostilities for marginal tactical gains, which would, at most, offer negligible advantages, while simultaneously giving the arguments to Russia to invade the country.[72]

Over the years, specialists in Russian disinformation have attempted to sway the Ukrainian populace through the strategic dissemination of "targeted messaging". Nevertheless, these efforts proved ineffectual in the face of the egregious war crimes perpetrated by Russian forces, exemplified by the events in Butcha.

[71] MARAHRENS, Sönke "The Russia-Ukraine Conflict from a Hybrid warfare perspective – A year in the war" (2023). https://tdhj.org/blog/post/russia-ukraine-hybrid-warfare/.
[72] MILANOVIC, Marko "When did the Armed Attack against Ukraine become 'Imminent'?" (April 2022), EJIL: Talk.

4.3- The question of imminence

We mentioned before article 51 of the UN Charter, and the statement is unequivocal, specifying that the right to self-defence "arises" solely in response to an armed attack; self-defence is not applicable to an attack that is hypothetical. In this context, an assessment of imminence necessitates consideration of the adversary's capabilities and objectives. Absent corresponding intentions, an attack cannot be deemed imminent solely based on the adversary's capabilities.

Imminence constitutes a crucial element of the requirement for self-defence, encompassing aspects of intention and causation. As stated by MICHAEL SCHMITT "the correct standard for evaluating a pre-emptive operation must be whether or not it occurred during the last possible window of opportunity in the face of an attack that was almost certainly going to occur."[73]

The Community of Interest for Strategy and Defence within the Center of Excellence Countering Hybrid Warfare documented overt demonstrations of military techniques in Ukraine, ascribed to the arsenal of hybrid warfare tactics deployed within sub-threshold contexts. [74]These methods encompassed the targeting and exploitation of systemic weaknesses to manipulate decision-making processes or destabilize and intimidate Ukrainian society.

However, we can confirm that Russia has the capacity to do this attack, so the uncertainty remains in the case of the State's intentions. Indeed, we are delving into subjective intentions, as there is no alternative method to envision the imminence of an event stemming from human agency. In this case, it is relatively feasible to humanize the abstract entity of the Russian state, given that Vladimir Putin singularly made all pivotal decisions.

Considering his "history of waiting until the last possible moment to make a decision, constantly re-evaluating his options", it is highly plausible that Putin remained uncertain of his decision until the morning of February 24th. [75] We saw before the situations from

[73] SCHMITT Michael N., "Pre-emptive Strategies in International Law", 24 MICH. J. INT'L L. 513 (2003), p.535.
[74] PORTER, Patrick "Out of the Shadows: Ukraine and the Shock of Non-Hybrid War" (2023), Journal of Global Security Studies.
[75] MILANOVIC, Marko "When did the Armed Attack against Ukraine become 'Imminent'?" (April 2022), EJIL: Talk.

Crimea 2014 to 2022, where we can consider that the attack began in different moments. This is not categorically the answer for a possible justified self-defence by Ukraine, but it certainly raises questions for the future. From now on, this undefinition can result in the use of pre-emptive self-defence deriving from cyberoperations, that could possibly indicate that an armed attack is being carried out.

Chapter V- The Russia-Ukraine conflict and the importance of adaption

5.1- Consequences of the Ukrainian war in the cyber domain

The significance of alliances has been underscored by Ukraine's cyber efforts. Consequently, several nations have enhanced their cyber diplomacy ventures by fostering, expanding, and reinforcing partnerships. Throughout the conflict in Ukraine, a series of cyber drills have been conducted, serving to underscore the collaborative nature of these exercises. Notably, in February 2023, France hosted ORION 23, [76]the largest event of its kind. With the involvement of 14 ally countries, ORION 23 constituted a multidomain exercise. Leveraging partnerships with at least 23 nations, the United States has executed over 50 "hunt-forward" operations across 75 networks by the midpoint of 2023.

The governments of Russia and Ukraine, along with the non-state organizations aligned with them, have been engaged in a competition for dominance over the narrative pertaining to the conflict and its progression within the realm of information dissemination. The authorities of both Russia and Ukraine, alongside non-state entities aligned with their respective interests, have been actively competing to shape and control the narrative regarding the ongoing conflict and its developments within the information domain. [77]

Cyber activities, encompassing influence-seeking aims and psychological impacts, possess the capacity to escalate as long as Russia persists in its unlawful warfare. The intense cyber and information warfare between Russia and the Western nations is likely to persist even if Russia were to cease hostilities and withdraw from Ukraine.

Furthermore, the example set by Russia highlights the imperative for rapid regeneration of cyber capabilities. Even during periods of peace and relative stability, U.S. Cyber Command has encountered challenges in restoring its force to full capacity. Consequently, efforts have been undertaken to develop more cost-effective and

[76]See Ministry of the Armed Forces, "Orion 23 Press Kit", February 2023, p.11, https://www.defense.gouv.fr/sites/default/files/operations/20230228_Press_Kit_Orion.pdf. , consult.10/Mar/2024.

[77] AUSTIN, Greg and Natallia KHANIEJO, "Impact of the Russia–Ukraine War on National Cyber Planning: A Survey of Ten Countries" (2023), The International Institute for Strategic Studies, pp.13-14.

disposable infrastructure and tools. [78] These challenges are likely to be exacerbated during a major conflict.

Their primary task is to reassess assessments of the adversary's offensive cyber capabilities in light of the constraints and challenges presented by Russia's actions in Ukraine. Consequently, cyber defenders must question whether they have overestimated the potential for their adversaries to employ cyber operations as a means of prevailing in future conflicts. For instance, American officials have harboured longstanding concerns regarding the possibility of a rival exploiting or disrupting American weaponry during times of conflict. Nevertheless, it appears that Russian forces have not inflicted serious compromises on American systems, despite encountering many of the same systems on the Ukrainian battlefield.

Experts, diplomats, and legal scholars universally acknowledge that, in principle, cyberspace is subject to regulation by international law. Nevertheless, there has been protracted and unfruitful debate concerning the mechanisms of its application, particularly regarding the determination of when cyberattacks reach a threshold of severity warranting classification as acts of war.

The paramount insight gleaned from this discourse is that several major cyber powers appear to have reached a consensus that offensive cyber operations conducted during periods of peace, even those extending beyond mere intelligence gathering, do not invariably constitute acts of war or armed attacks[79]. Consequently, it remains plausible that an assault employing cyberspace as the primary means of executing a strategic strike, resulting in significant casualties, could be categorized as an armed attack. NATO, for example, has adapted its strategy in recent times to incorporate this concept. [80]

While such an approach may appear advantageous from a policy perspective, it nonetheless sets a relatively high threshold for offensive cyber activities to be regarded seriously as acts of war. Moreover, it somewhat diminishes their normative and deterrent

[78] BATEMAN, Jon "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications" (2022), Carnegie Endowment for International Peace, pp.52-56.
[79] LEVITE, Ariel E. "Integrating Cyber into Warfighting: Some Early Takeaways from the Ukraine Conflict" (2023), Carnegie Endowment for International Peace, pp.9-12.
[80] Refer to Jennifer Hansler for decisions made on this subject during the NATO summit in June 2022, "NATO Agrees Cyberattacks Could Amount to Armed Attacks and Lead to Invocation of Mutual Self-defence Clause," CNN, June 14, 2021.

efficacy by deferring the determination of whether these criteria have been satisfied to post facto, case-by-case deliberation. [81]

The measures implemented prior to the conflict to aid in the development and execution of a national cyber strategy have significantly improved the resilience of Ukrainian networks. Information sharing and interoperability represent the principal areas where diplomatic efforts to support cybersecurity should be focused. The U.S. administration ought to accelerate its processes to inform its allies about vulnerabilities concerning information sharing. [82]

Cyber activities are constrained by a commitment issue: current utilization is limited by concerns over potential future losses. This logic underscores the preference for employing tangible methods such as artillery and missile strikes, rather than engaging in actions whose impacts are more challenging to quantify. [83]

5.2- EU and NATO aligned to combat cyberthreats in Ukraine

It is imperative that both the EU and NATO collaborate closely to effectively equip Ukraine for prospective membership. The Alliance will play a pivotal role in providing training to Ukraine, aimed at ensuring alignment with NATO standards.

In this context, the European Union's comprehensive arsenal for countering hybrid threats, which encompasses strategies to address cyberattacks, disinformation campaigns, and related tactics, assumes particular significance. Given that both the EU and NATO accord high priority to enhancing resilience against such threats, it is imperative for them to collaborate in exploring optimal avenues for extending support to Ukraine in fortifying its resilience capacities.[84]

Cyberattacks targeting Ukraine's allies, including Poland, Latvia, Finland, and Denmark, have proliferated since the onset of the conflict in Ukraine. According to

[81] TSAGOURIAS, Nicholas and Russell BUCHAN,2023, "Research Handbook on International Law and Cyberspace", *2nd ed,* Edward Elgar, pp. 519-521.
[82] MUELLER, Grace B. et al, "Cyber Operations during the Russo-Ukrainian War", Center for Strategic and International Studies (2023), p.14-17.
[83] GRAY, Colin S., "Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century", Strategic Studies Institute, US Army War College (2011), p. 47-53.
[84] ZANDEE, Dick and Dijkman, Mik "The EU and Ukraine Towards a new security and defence relationship" (2023), Cligendael, Netherlands Institute of International Relations. https://www.pubaffairsbruxelles.eu/opinion-analysis/the-eu-and-ukraine/, consult. 11/Feb/2024.

BOUDREAUX-DEHMER, NATO's chief information office, "we haven't seen the attack that can trigger Article 5 yet". If one does exist, though, NATO is able to take into account many alternatives for how to counter it, not just in the same way that it was attacked but also in a new way. "With regard to Article 5, there is a great deal of flexibility", he continued. [85]

The European Union is deliberating the creation of a novel EU cybersecurity reserve comprising incident response services sourced from private sector enterprises. This reserve would be mobilized upon request by a member state in the event of a significant or widespread cybersecurity incident, thereby augmenting the EU's collective capacity to address such threats effectively.[86]

On the global stage, Russian disinformation and propaganda campaigns have exerted considerable influence in the realm of cyberattacks and information warfare. Allegations abound regarding the exploitation of cyberspace by the Russian government and its affiliates to disseminate misinformation, manipulate narratives, and advance their geopolitical agendas.

In April 2023, following the discovery of a leak of highly classified military documents about the conflict in Ukraine, the Pentagon moved quickly to reassure allies and gauge the extent of the material exposed. The classified documents span a variety of topics, including the circumstances under which Russian President Vladimir Putin might use nuclear weapons, and range from briefing slides outlining Ukrainian military positions to assessments of international support for Ukraine and other sensitive topics.[87] This indicates a clear fragility for the western cyber defence, high levels of espionage that could have led to the fall of the entire Ukrainian defence.

The European Union's cyber defence policy is founded on four primary pillars, which encapsulate a diverse array of measures designed to enhance the EU's and its Member States' capabilities in identifying, preventing, and mitigating cyberattacks: (i) Take coordinated action to improve EU cyber defence; (ii) Protect the defence industry; (iii)

[85] NATO's chief information officer, Manfred Boudreaux-Dehmer, told Recorded Future News during a cybersecurity conference in Munich (February, 2024). https://therecord.media/nato-cio-ukraine-war-cyberdefense-russia, consult. 25/Mar/2024.
[86] See the EU Cyber Solidarity Act in:https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity, consult. 06/ Feb/2024.
[87] See in: https://edition.cnn.com/2023/04/11/politics/pentagon-documents-ukraine-war-assessment/index.html , consult. 15/Mar/2024.

Make an investment in cyber defence tools. (iv) Collaboratively Addressing Common Challenges.[88]

Recently, we have made significant progress in the direction we were pursuing, building upon all the arguments previously articulated. To bolster the identification, anticipation, and management of cyberthreats and incidents, the Cyber Solidarity Act aims to fortify solidarity across the European Union. To establish a European Cybersecurity Alert System, a network of national and cross-border Cyber Hubs must be erected. These hubs will utilize cutting-edge infrastructures and capabilities, such as advanced data analytics and artificial intelligence, to promptly identify cyber incidents and threats. [89]

The conflict between Russia and Ukraine has precipitated numerous changes, reverberating across various facets such as the framework of international security, the dynamics of shaping a new global order, the deepening ties between China and Russia, the efficacy of drones in military operations, the resurgence of nuclear posturing, the exacerbation of global food shortages, the energy constraints experienced in Europe, and other significant shifts. Additionally, there is a pressing need to enhance cooperative strategies in this domain to effectively mitigate cyber threats and safeguard collective security interests. [90]

[88] EU Cybersecurity Policies in https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies, consult in 25/ Feb/2024.
[89] European Comission, Commission welcomes political agreement on Cyber Solidarity Act, (March 2024), see in : Political agreement on Cyber Solidarity Act (europa.eu),consult.23/Mar/2024.
[90] Guchua, Alika and Zedelashvili, Thornike, "Challenges arising from cyber security in the dimension of modern global security (on the example of the Russia-Ukraine war)" (2023), pp.6-9.

Chapter VI- Conclusion

Throughout the course of this study, we have recognized the escalating significance of International Organizations in shaping the democracies and societies of the world. Concurrently, we have discerned that shared policies and consensus among these organizations facilitate advancements in the defence capabilities of nations.

Moreover, developed areas where efforts to strengthen cooperation have been insufficiently pursued. From the standpoint that International Organizations should judiciously exercise their legal personality to safeguard the interests of their members, they bear accountability for their actions. They are bound by their constitutive instruments and by the overarching principles of international law.

Subsequently, we delved into an analysis as the Common Foreign and Security Policy serves as the cornerstone for security and cooperation within the European space. Our examination led us to the determination that the EU possesses distinct competences for the implementation of the Common Foreign, Security, and Defence Policy, as stipulated in Article 2(4) of the TFEU.

Afterwards, in conjunction with the aforementioned one of the conclusions, was that the European Union budget is not intended to be spent in defence or military measures, as incorporated in article 41(2) TFEU. The concept of burden sharing has been extensively discussed, particularly in light of the direct impact of the conflict in Ukraine on European nations. Consequently, Allies have undertaken efforts to augment defence spending, enhance the capacity of their armed forces, and actively engage in operations, missions, and related procedures within the framework of the Alliance.

Thus, our attention was turned to the concept of "strategic autonomy" and its introduction into the geopolitical discourse by France. This concept advocates for a sovereign Europe capable of self-defence without reliance on external actors. However, our analysis revealed that the majority of EU members continue to place their trust in the United States and perceive it as the primary regulator of Western countries. While acknowledging the undeniable military power of the U.S., our perspective leads us to the conclusion that NATO, without U.S. involvement, would lack the necessary influence and capacity to address emerging conflicts effectively.

It was our goal to contemplate the ramifications of the Ukrainian conflict on the cyber domain. Despite being a relatively nascent facet of international law, cyber threats have become increasingly intricate amid this conflict. We conclude that the day the Russia-Ukraine aggression started depends on the subjective element, that is the intention from the Russia´s leader to perpetrate the attack. Without this clarification, it seems impossible to legitimately use pre-emptive self-defence.

Finally, we also scrutinized whether a cyber-attack aligns with the definition of an armed attack. In this regard, we concluded that the assessment of whether these criteria have been met necessitates *post facto*, case-by-case deliberation. We are truly in the era of hybrid warfare, NATO and EU have to join forces to create defence mechanisms that quickly identify cyberthreats and immediately eliminate them. Cyber defence in Ukraine has played a pivotal role as a crucial defensive barrier. Nevertheless, we maintain that the EU should possess the capability to actively establish itself as a predominant force in cyberspace, rather than merely reacting to evolving circumstances.

In conclusion, the cyber domain emerged as an unpredictable element in the Ukrainian conflict, catching Ukraine and all NATO allies off guard, who were anticipating the onset of a conventional conflict to officially deem it an act of aggression. Russia initiated a campaign of misinformation aimed at swaying public opinion in Ukraine in favour of Vladimir Putin. The challenge facing NATO and the EU lies in enhancing coordinated action in the cyber sphere to empower Ukrainian resistance in this domain. As defenders of democratic values, they can´t let an important ally fall behind, so the support of Ukraine is vital for a demonstration of strength and readiness from the EU and U.S. This will make an impact for other countries, especially in Asia, but will continue to legitimize the internal guidance of Member States that will be able to financially, humanitarianly and logistically continue to give a cohesive response alongside the Union and the North Atlantic Alliance.

Bibliography

AMERASINGHE, C.F.,2005, "Principles of Institutional Organizations",2nd ed, Cambridge studies in international and comparative Law, pp. 16-21.

AUSTIN, Greg and Natallia KHANIEJO, "Impact of the Russia–Ukraine War on National Cyber Planning: A Survey of Ten Countries" (2023), The International Institute for Strategic Studies, pp.13-14.

BATEMAN, Jon "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications" (2022), Carnegie Endowment for International Peace, pp.52-56.

BORDIN, Fernando Lusa, 2023, "The Quest for International Legal Status: On Finn Seyersted and the Challenges of Theorizing International Organizations Law", European Journal of International Law, Volume 34, Issue 1, pp.5.

COGAN, Jacob Katz; Ian HURD and Ian JOHNSTONE, 2016, "The Oxford Handbook of International Organizations", *1st Oxford* University Press, pp. 115-118.

COLIBASANU Antonia, "Decision-making and disarray in the EU", July 2016, see in https://www.euractiv.com/section/euro-finance/opinion/decision-making-and-disarray-in-the-eu/, consult in 15/Feb/ 2024.

DABROWSKI, Marek, "To become a geopolitical player the European Union needs Treaty change" (2024), Bruegel.

DAUGIRDAS, Kristina, 2020, "International Organizations and the Creation of Customary International Law", The European Journal of International Law Vol. 31 no. 1, p.7.

D´OLIVEIRA MARTINS, Margarida Salema e Afonso, 1996, "Direito das Organizações Internacionais", Vol. I, 2ª ed, Lisboa: AAFDL p.9.

LEVITE, Ariel E., "Integrating Cyber into Warfighting: Some Early Takeaways from the Ukraine Conflict" (2023), Carnegie Endowment for International Peace, pp.9-12.

FAIRLESS, Tom, "How War in Europe Boosts the U.S. Economy", The Wall Street Journal in https://www.wsj.com/economy/ukraine-war-europe-american-economy-654ca41b, consult, 18/ Mar/2024.

FILIPEC Ondřej, "The cooperation between EU and NATO in response to hybrid threats – A retrospective analysis from the institutionalist perspective", Slovak Journal of Political Sciences, Volume 23, No. 1, 2023, pp.43-47.

GNESOTTO Nicole, "La puissance et l'Europe", Paris: Presses de Sciences Po, (1998).

GONZÁLEZ LAYA, Arancha, "La EU, entre lo inevitable y lo impossible", April 2024, Abc.es.

GRAY, Colin S., "Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century", Strategic Studies Institute, US Army War College (2011), p. 47-53.

GUCHUA, Alika and Zedelashvili, THORNIKE, "Challenges arising from cyber security in the dimension of modern global security (on the example of the Russia-Ukraine war)" (2023), pp.6-9.

PAIVA DA CUNHA, Agostinho, “Acerca do Conceito Estratégico da NATO. A Caminho de Lisboa, uma Nova Estratégia para o Século XX”, Repositório Comum,31 de janeiro de 2010, p.124-125.

POLCIKIEWICZ, Zdzislaw, “Cooperation between NATO and the European Union for shaping international security”, The Copernicus Journal of Political Studies, 2019, Pp. 75-82.

PORTO LOPES, Manuel e Gonçalo ANASTÁCIO (Coordenadores), 2012, “Tratado de Lisboa Anotado e Comentado”, Almedina, p.204-207.

PORTER, Patrick “Out of the Shadows: Ukraine and the Shock of Non-Hybrid War” (2023), Journal of Global Security Studies.

JENKS, Clarence Wilfred, 1962, “The Proper Law of International Organizations”, Vol.2, California University.

JUNCOS, Ana E. and Sophie,VANHOONACKER, “The Ideational Power of Strategic Autonomy in EU Security and External Economic Policies”, Journal of Common Market Studies (2024), pp.1-18.

KLABBERS, Jan, 2015, “An Introduction to International Organizations Law”, 3rd ed, Cambridge University Press, pp. 2-6.

KOSTAKAROS, Mikhail, “Guest Editorial”, European Foreign Affairs Review 23, no. 4 (2018), pp. 436–437.

KOUTRAKOS, Panos, "The European Union´s Common Foreign and Security Policy after the Treaty of Lisbon", Published by the Swedish Institute for European Policy Studies, Report No. 3 May 2017, pp.16-31.

MARAHRENS, Sönke "The Russia-Ukraine Conflict from a Hybrid warfare perspective – A year in the war" (2023). https://tdhj.org/blog/post/russia-ukraine-hybrid-warfare/.

MCINNIS Kathleen and Daniel FATA, "From Burden Sharing to Responsibility Sharing", Center for Strategic and International Studies (2023), p.6-9.

MILANOVIC, Marko "When did the Armed Attack against Ukraine become 'Imminent'?" (April 2022), EJIL: Talk.

MUELLER, Grace B. et al, "Cyber Operations during the Russo-Ukrainian War", Center for Strategic and International Studies (2023), p.14-17.

NAUTA, David, 2016, The International Responsibility of NATO and its personnel during military operations, Doctoral Thesis, Radboud University Nijmegen, pp. 65-69.

RADANLIEV, Petar "Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing" (2024), Journal of Cyber Security Technology.

RANGEL DE MESQUITA, Maria José, 2011, "A Actuação Externa da União Europeia depois do Tratado de Lisboa", Almedina, pp. 394-414.

SCHMITT Michael N., "Pre-emptive Strategies in International Law", 24 MICH. J. INT'L L. 513 (2003), p.535.

THOMSON, Catarina P., “Foreign policy attitudes and national alignments in times of Chinese and Russian threats: public opinion across three NATO members”, The RUSI Journal 167: 2, 2022, pp. 24–37.

TOCCI Nathalie, “How the war in Ukraine has transformed the EU”, November 2023 https://www.socialeurope.eu/how-the-war-in-ukraine-has-transformed-the-eu.

TSAGOURIAS, Nicholas and Russell BUCHAN,2023, “Research Handbook on International Law and Cyberspace”,*2nd ed,* Edward Elgar, pp. 521-522.

VON ACHENCACH, Jelena, “Too Little Politics in EU Defence Policy- The EU Arms Supplies to Ukraine from the Perspective of Budgetary and Constitutional Law”, Verfassungs blog on Matters Constitutional, March 2022.

WESSEL, RAMSES A. et al, “The future of EU Foreign, Security and Defence Policy: Assessing legal options for improvement”, European Law Journal, Vol 26, 2021, pp.374-388.

ZANDEE, Dick and Dijkman, Mik “The EU and Ukraine Towards a new security and defence relationship” (2023), Cligendael, Netherlands Institute of International Relations. https://www.pubaffairsbruxelles.eu/opinion-analysis/the-eu-and-ukraine/, consult. 11/Feb/2024.

Legislation, Jurisprudence and Official Documents

Advisory Opinion stated by the ICJ in the case Reparation for Injuries Suffered in the Service of the United Nations (in International Court of Justice, Reports and Advisory opinions, 1949, p.174 ss).

Council of the EU, 14 November 2016, Council conclusions on implementing the EU Global Strategy in the area of Security and Defence.

European Council. (2013) Council Conclusions. 19–20 December 2013. See in: pdf (europa.eu), consult 10/ Mar/2024.

European Parliament resolution of 22 November 2012 on Cyber Security and Defence (2012/2096(INI)

International Court of Justice, Reports and Advisory Opinions, 1949.

Treaty on European Union

Treaty on the Functioning of the European Union

UN Charter, 1945