Framing Artificial Intelligence: The Interplay between AI Policies and Security in the European Union

July 2022

GUID: 2571555L

DCU ID: 20109750

CU ID: 15481502

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 20797

Supervisor: Professor Timothy Peacock

Date of Submission: 27th of July 2022

Table of Contents

Abstract

Artificial Intelligence (AI) is increasingly more embedded into our lives. Hence, the literature that explores the new technology is vast. However, there is a lack of resources that address how the technology is framed at the level of the European Union (EU). Specifically, few studies assess whether there are differences between the institutions' framing of AI policies. Scholars also overlook the potential implications of AI for the security of the Union. The present study seeks to fill in these gaps by examining how the European Commission (EC) and the European Parliament (EP) frame AI security policies. The dissertation also investigates whether there are differences between the institutions in how AI security policies. To do this, the research is split into two main sections. The first section explores how the two institutions frame AI security using a combination of the *Policy Framing* approach and qualitative content analysis. The unique research design was used on 10 official documents released by the EC and EP between 2017 and 2021. On the one hand, the outcome indicates that the EC frames AI policies through the perspective of three security areas, namely economic, social and political. On the other hand, the EP's framing of AI policies reckons the same areas of security, also adding the military perspective. The second section introduces a comparative analysis of the frames. The comparison takes place against three elements: definition of security, definition of AI, and engagement with the security sectors. The elements were drawn as a result of empirical qualitative analysis. The author chose these elements because they are considered the best in assessing the interplay between AI and security in the EU. The output of the analysis demonstrates that there are clear divergences in how the EC and the EP frame AI security policies.

Keywords: *Artificial Intelligence, European Union, security, framing, European Commission, European Parliament*

Acknowledgments

I would like to acknowledge and give my warmest thanks to my supervisor, Timothy Peacock, who guided me and supported me throughout all the stages of the writing process. Your patience and feedback were invaluable. This journey wouldn't have been possible without my parents and grandma, Sabina, Octavian and Constanța, who never hesitated to show their love, compassion and understanding when writing my final project. Their belief in me kept my head and spirits high.

My gratitude also goes to Jelena, who's been a tireless pillar of emotional, moral, and academic support. Her presence in my life is invaluable. I would like to extend my sincerest thanks to my best friend, Andra, for your unwavering faith in me and continuous encouragement over the past 14 years. I am also thankful for my dearest friends Rhys, Marisia, Maria, Klara, Leticia, Jelle, Elene, Fateh, and Ibrahim. You all impacted and inspired me all throughout my Master's.

Lastly, I would be remiss in not mentioning my professor from Cluj-Napoca, Natalia, without whom I wouldn't have reached this point, and Iuliana who pushed me up until the end and never stopped believing in me.

Introduction

Research Puzzle

The present security landscape is diverse and dynamic. As such, it spans a large spectrum of threats that require high levels of adaptability, resilience, and readiness- from an individual to a supranational level. Therefore, proper management of resources and capabilities is a necessity. Unequivocally, Artificial Intelligence (AI) is one of the most considerable means to address widespread security risks. AI is one of the latest innovations that is set to revolutionize the future of the world. On the one hand, AI technology is a catalyst of benefits for society due to its wide applicability across sectors. On the other hand, AI can easily become a security threat due to its irregular evolution and uncertain features. To cope with the complexity of the current security environment, AI requires effective regulation. Global superpowers, such as the United States (US) and China, have already made concrete steps to regulate the governance of AI. The European Union (EU) followed suit; its efforts to stipulate AI governance started in 2017 and are still progressing. The EU has a unique governance structure based on a small number of institutional bodies. Two of the most important institutions are the European Commission (EC) and the European Parliament (EP). Both worked extensively to research the new technology and develop a unique approach to implement it across the Union. Yet, it is unclear whether the institutions have different or similar approaches to the technology. The consequences of a potential misalignment for the security of the Union are also unknown.

Research Question

In the context outlined above, the main Research Question of this paper is *"To what extent are there differences between the EU institutions in the framing of Artificial Intelligence security policies?"* To address the question,

this paper analyzes 10 official documents released by the EC and the EP for the period 2017 to 2021.

Main argument

This research argues that there are clear divergences between the EC and EP in how they frame AI security policies. The clear divergences stem from how each institution conveys its understanding of the effects of AI on security. In other words, the manner in which the institutions frame AI effects on security indicate inconsistency in how they define security, AI, and how they engage with the security sectors. As such, the construction of the argument takes place in two parts. First, the author created a unique set of frames to set the ground for the analysis. To do so, the research design of the paper combined the *Policy Framing* approach developed by Rein and Schon and qualitative content analysis. As a result, the author observed the following. On the one hand, the EC frames AI policies through the perspective of three security areas – economic, social, and political. While the EP policy documents also account for these security areas, they also incorporate the military security perspective to a great extent. From the outset of the frames, the differences between the institutions are visible. Second, the author conducted a comparative analysis of the frames to better assess the similarities and differences between the institutions' AI framing of security policies. The comparison was conducted against three elements. These elements are the definition of security, the definition of AI, and engagement with security sectors. The elements were identified through an empirical qualitative analysis of the frames. Even though the elements may not be representative of all existing similarities and differences between the institutions' framing of AI security policies, they serve the purpose of this analysis. They can adequately showcase the interplay between AI and security. Moreover, the variables can easily represent the initial groundwork for future studies. To provide some examples in both cases, neither institution defined what is meant by 'security'. The interpretation of the word

was up to the author of this paper who determined its meaning through the contexts of the official documents. The absence of a clear conceptualization of 'security' hinders proper management of the technology and already questions the governance structure of the Union. As a difference, whereas both institutions outline the definition of AI, they engage differently with it. EC rarely refers to the technological features of AI, whereas the EP places great emphasis on the state-of-art of the technology in the delivery of its provisions. Finally, the analysis determined that the starkest difference between the institutional bodies is the absence of the military perspective from the EC's side. The international representation of the Union happens through the EC. Without framing AI policies from a military security perspective, the EC places the Union in the position of a weak actor. Furthermore, AI is already used for the enhancement of military and defense capabilities. Hence, concrete lines of action are needed in this sense, especially in the context in which the EU wants to obtain strategic autonomy.

Roadmap

For an accurate representation of the Research Question, this paper is organized into three chapters: Literature Review, Theory & Research Design, and Findings. The first chapter, **Literature Review**, looks at the contributions of authors from the sphere of AI effects in politics. The field is broad and comprehensive. As such, the author focuses on the contributions that are in line with the Research Question of this paper. Therefore, the secondary resources are organized into three categories: Governance of AI, AI implications in security, and AI in the EU sphere. The final section of the chapter highlights the gaps that the present research attempts to cover. First, the research showcases how other institutions, frame AI policies other than the EC. Second, the dissertation contributes to the concept of governance of AI. The novelty is that this research looks at AI governance from a security perspective. The study also gives insight into how the EC and the EP frame AI security policies, which was

not attempted previously. Finally, the empirical contribution of this research stands in the comparison between EC and EP's frames of security.

The second chapter, **Theory & Research Design**, starts with the introduction of the conceptual framework used in this paper. Consequently, the **Theory** section briefly outlines the general *Framing* theory, followed by the *Policy Framing* approach developed by Rein and Schon. More specifically, the paper engages with the criteria for the construction of a 'rhetorical frame'. The conceptual framework is also used to draw three alternative hypotheses. The next section, **Research Design**, introduces the unique model of analysis employed in this research. For the construction of the frames, the author uses a combination between the criteria of 'rhetorical frames' and qualitative content analysis. For the comparison of frames, the author conducts an empirical qualitative analysis that returns three elements: the definition of security, the definition of AI, and engagement with the security sectors. Based on the elements, the author was able to determine the similarities and differences existent between the EC and EP in how they frame AI security policies.

The last chapter, **Findings,** is the most extensive part of this research. The chapter is organized into three subsections: **Framing**, **Analysis,** and **Discussion**. The **Framing** segment dives into a comprehensive presentation of the frames derived from the model analysis for both the EC and the EP. The **Analysis** section represents the critical delivery of this study. It consists of the comparison of frames, performed against the three elements identified through the empirical qualitative analysis. In the display of similarities and differences, the author employs a critical assessment to determine the initial implications of a potential misalignment. The **Discussion** section highlights the implications of this research, both empirically and academically. The section also introduces the limitations of the research and recommendation for future studies. Having this outline of chapters, the dissertation proceeds with the first chapter, **Literature Review**.

Chapter 1. Literature Review

The Research Question of this paper is *To what extent are there differences between the EU institutions in the framing of Artificial Intelligence security policies?* Therefore, the intention of the present Literature Review is to provide the analytical foundation for how Artificial Intelligence (AI) is framed at the level of the European Union (EU) institutions. As such, the chapter is organized as follows. First, the section of **Problems and Debates** introduces the current debates existent in the academia circles on the topic of AI's applicability in politics. The second segment, **Questions and Hypotheses**, is organized in three specific research streams: **Governance of AI**, **AI implications in security**, and **AI effects in the EU**. The chapter concludes with the **Gaps and Contributions** section. It delineates the lacunas existent in the body of literature and how the present dissertation attempts to bridge them.

1.1 Problems and debates

The "governance of Artificial Intelligence (AI) is a significantly underdeveloped area" (Taeihagh, 2021, p. 1). Hence, one of the most important purposes of this Literature Review is to provide the basis that can showcase the originality and contributions of this dissertation for a better understanding of AI's applicability in politics. This section introduces the main problems and debates currently existent in the literature that is in line with the Research Question of this paper. The proliferation of academic works focused on Artificial Intelligence (AI) started after the so-called 'AI Winter', in 1987 (*AI Winter*, 2021). The vast applicability of the innovative technology across multiple sectors raised the interest of scholars. Given this context, keeping track of the proliferation of studies about AI became progressively hard (Oke, 2008, p. 1). Sunday Oke attempted to produce a systematic literature review that encompasses all the relevant scholarly works in the AI field. To the extent of this research, such an attempt has not been reproduced nowadays. However, the

literature pertinent to this study is appraised in the present review.

As such, the focus is placed on the advent of AI in the political sphere. Research surrounding the effects of AI on politics around the world is rather new. The interest in the applicability of AI in politics gained momentum around 2012. The rapid expansion, along with the privatization of AI gave rise to several benefits and drawbacks. Such a context called for immediate action from the side of policymakers. Consequently, in the first half of 2018, a growing number of countries released national AI strategies (Taeihagh, 2021a, p. 138). The strategies are designed to address the challenges and risks associated with AI, how are the governments going to address them while also having a prolific introduction of the technology into society. In conjunction, two factors -the swift progress in the development of AI and its introduction in politics- provide the foundation for the interest of scholars in the area of AI implications in politics.

Given the novelty of the topic, the literature is relatively scarce. Nonetheless, the kernel of these scholarly works is to showcase the applicability of AI in various governmental sectors and the risks entailed with it, most of its ethical nature. Indeed, much of the debate revolves around the revolutionary changes brought by AI, its unpredictability and uncontrollability, and how effective management is needed to address these challenges (Butcher & Beridze, 2019; Buiten, 2019; Alaca, 2019). The consensus among scholars is that AI will continue to shape the outlook of future societies. For example, Cath et. al argue that if societies are gradually more "information mature", the reliance on AI technologies will increase (Cath et al., 2017, p. 2). Similarly, Efthymiou et al. affirm that at its current stage, AI cannot be disregarded, as "it is set to transform the society, the economy and politics" (Efthymiou et al., 2020, p. 2). It is unclear, nevertheless, how individuals can use AI in their policies efficiently, and much of the debate concerning this issue is rather speculative. Alan Dafoe stated in an interview that the governance of AI will be a difficult endeavor due to three reasons: "[...] the strategic importance of the

technology, its diverse applications, and the uncertainty associated with its developmental trajectory." (A. Dafoe, personal communication, 2018). Indeed, the uneven evolution of AI is another reason for concern, especially if policymakers want to regulate it efficiently.

Notwithstanding these concerns, few scholars focused their research on how AI policies are framed, especially if the main area of interest is the European Union (EU). More particularly, the implications of AI policies in security were previously assessed by a handful of scholars in countries such as China, the United States (US), and Russia. By contrast, the number of resources addressing the approach of the EU in this regard is rather low. Furthermore, the EU has a unique structure of governance that allows for the division of duties and responsibilities among its institutions. Consequently, the examination of how security policies are treated in the EU sphere is worthwhile for two reasons. First, it showcases the intricacies entailed in regulating AI efficiently in all areas of security, from economy to military and defense. Second, it uncovers the potential implications that might arise due to a discrepancy between the main institutions. The next section explores the scholarly works that provide the foundation for this dissertation.

1.2 Questions and hypotheses

As mentioned previously, the applicability of Artificial Intelligence (AI) in politics opened the avenue for several research streams. Providing an overview of each sub-branch of AI in politics goes beyond the scope of this paper. Rather, consistent with the Research Question of the dissertation, this section addresses three lines of research approached by scholars in the sphere of AI in politics, which are following: governance of AI, AI implications in security, and finally how AI is treated in the EU sphere of influence. Evaluating the literature from these three categories is essential as it sets the ground for the contribution of the present research.

1.2.1 Governance of Artificial Intelligence (AI)

At the center of this topic is a consensus amongst scholars, that the governance of AI will prove to be difficult. Nonetheless, the accurate comprehension of the subject requires the delineation of some pivotal elements. First, the concept of 'governance' has been extensively researched by scholars, which predominantly refers to "all the processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, [...] or territory, and whether through laws, norms, power or language." (Bevir, 2012, p. 1) Second, the emergence of technology and its embeddedness into society practices gave rise to a new field of study, namely the 'governance of technology'. The 'governance of technology' is a diverse bailiwick that follows the interplay between concepts and ideas drawn from political, economic, and social sciences and Science and Technology Studies (Ulnicane et al., 2021, p. 160). Jasanoff highlighted two essential characteristics of the 'governance of technology'. The first is that technologies are not used just for 'achieving practical ends' but facilitate the creation of 'more liberating and meaningful designs for future living.' (Jasanoff, 2016, p. 242) The second is that "technological choices are, [...], intrinsically political: they order society, distribute benefits and burdens, and channel power." (*Ibid.*, p. 243)

Outlining the concepts of "governance" and "governance of technology" is relevant for the assessment of the literature that addresses the governance of AI. AI is a technology that, according to academic works, is difficult to regulate due to two general factors: the idiosyncrasies entailed to AI; reaching a consensus between the private and public sectors as to what interest should AI serve. Allan Dafoe argues in an interview that, on the one hand, the design of good governance of AI will entail thorough attention to the technical landscape of AI (A. Dafoe, personal communication, 2019, p. 122). On the other hand, the ideal governance of AI will encompass norms, initiatives, and policies that are based on principles such as fairness, transparency, and privacy and that are developed jointly with multilateral organizations (*Ibid.*). The author also

discussed the potential risks associated with a machine that exceeds or is equivalent to human capabilities. These risks are not only of strategic nature (e.g. cyber warfare), but also of societal and economic concern (e.g. labor displacement, erosion of privacy, etc.) (*Ibid.,* p. 123). The bottom line argument of the author is that the key to a proper and functional framework for the governance of AI "will be striking a balance between private and public interests, and aligning firm incentives with the pursuit of the common benefit of humanity" (*Ibid.*, p. 125).

Taeihagh claims that despite the evident changes in the organization of the society brought about by AI, little was written on the governance of the new technology (Taeihagh, 2021b, p. 137). Thus, together with several authors, he launched a special issue that introduces the multifaceted challenges of the governance of AI (*Ibid.)*. In his article, Taeihagh touches upon a variety of issues surrounding the governance of AI. His core argument is that the unpredictability and complexity of AI are the main challenges to the elaboration of efficient policies that seek to regulate the new technology (*Ibid.*, p. 143). For example, from a technological perspective, the obscurity of Machine Learning (ML) algorithms raises concerns about ethics, transparency, accountability, and explainability, all of which are essential elements in the creation of a governance framework (Lim & Taeihagh, 2019; Mittelstadt et al., 2016). The opacity of ML algorithms is driven by security reasons, such as to prevent them from cyber attacks and to "safeguard trade secrets, [...]" (Carabantes, 2020; Goodman & Flaxman, 2017; Kroll et. al 2016). However, as Taeihagh himself argues, "the decision-making autonomy of AI significantly reduces human control over their decisions, creating new challenges for ascribing responsibility and legal liability for the harms imposed by AI on others." (Taeihagh, 2021b, p. 141) As solutions to the enumerated challenges, he proposes innovative governance approaches such as adaptive governance or hybrid governance (*Ibid.)*.

From an empirical perspective, Roxana Radu conducted an assessment

of different National Strategies on AI using hybrid governance as a framework. She argues that the priorities outlined in the strategies by governments represent "the basis for regulatory configurations and functional assignment of roles and responsibilities in policy-making."(Radu, 2021, p. 179) However, the AI industry is a largely privatized domain. Hence, through the lens of the conceptual framework, her findings suggest that the way forward for the governance of AI is to unite the political will and public resources with the industry interests (*Ibid.*, p. 190). The first key takeaway from her research is that the interests of the governments and industries converge (*Ibid.*). Second, the vagueness of the roles of the public and private sector, as well as the market-oriented approach and the prioritization of ethical guidelines are suggestive that hybridity is both desired in the governance of AI, but also an outcome of the fast AI developments (*Ibid.,* p 191).

Akin to this research, a handful of authors have looked at the governance of AI through the lens of the framing theory. However, despite adopting the same framework, the approaches taken by the authors are different. On the one hand, Ulnicane et al. argue that governance is in itself a frame that is used in policy discourses "as a way to overcome controversies surrounding AI development and use." (Ulnicane et al., 2021, p. 159) The scholars drew their argument after performing an analysis over 49 AI documents published in recent years (2016-2018) by both state and non-state actors. Their findings indicate that the present governance of AI is marked by a small number of large companies that hold the monopoly in the sector (*Ibid.*, p.171). The oligopoly of these companies is considered, among other factors, one of the main impediments to the consideration of societal needs and concerns (*Ibid.*). However, a governance frame is presented as the solution to address these problems, as it "assigns more active and collaborative roles to the state and society."(*Ibid.*) Notwithstanding the benefits of a governance frame, there are certain limitations to it that the authors are emphasizing which include the difficulties of reaching consensus or how vested interests are going to be treated

(*Ibid*.).

On the other hand, Gahnberg took a very interesting and unique approach to the subject. He argues for the scrutiny of the new technology's governance, AI should be understood as the creation of "artificial agents, [...]" that operate better in different contexts (Gahnberg, 2021, p. 194). Therefore, the challenge that the governance of AI should seek to address should be understood as one of material agency (*Ibid.*). From this perspective, the author proposes a conceptual framework that encompasses the properties of artificial agents "to systematically analyze governance across a vast range of AI applications."(*Ibid.)* The uniqueness of his study is twofold. First, he introduces the essential features of artificial agents (e.g. the creation of an AI system). Second, by drawing insights from the governance literature, Gahnberg frames the issue of the governance of AI as related to the material agency of artificial agents. By combining the two factors, he designs the conceptual framework for AI governance. The scholar demonstrated the applicability of the framework in all types of AI applications by using concrete and empirical examples of existing or emerging mechanisms (*Ibid.*, p. 195).

To conclude, AI is a technology that will be difficult to govern due to several factors. First, the continuous development and the various applications of AI represent a large spectrum of benefits that are meant to improve the quality of human lives. Nevertheless, concerns about ethical principles such as transparency, accountability, privacy, etc. are especially prevailing in the discourse on the governance of the new technology. Second, given its unpredictable and uncertain nature, the technical prospect of AI is another point of concern. The unclarity surrounding the building of an AI system (e.g. algorithm construction, management of databases necessary for the proper function of the system, etc.) can hinder the progress of perfecting the governance of AI. Furthermore, it can generate a high level of distrust between the public and the private sector, state or non-state actors. This leads to the last point, which is the convergence needed between a multitude of actors for a

proper governance of the technology. The majority of authors have pointed out how the interests and objectives of the state related to AI need to intersect with those of the private sector. This section showcased how, altogether, these factors make the endeavor of pioneering policies over AI-enabled technologies difficult and complex.

1.2.2. Artificial Intelligence (AI) implications in security

The implications of AI in security are multifarious, from the revolutionary technological development of armament to a possible rearrangement of the international system. Most of the literature that appraises the effects of AI in security, is approaching 'security' from a realist perspective. Elements such as 'balance of power', 'military capabilities', 'defense' etc. are all recurrent themes in the scholarly works on the topic. Fischer and Wegner (2021) argue that the discussion of AI in politics is focused on two main and interconnected research streams. The first course of study addresses AI governance, evaluated in the previous section. The second subject field highlights that the main security questions related to AI in politics are addressing how states are using the technology as a strategic resource in anticipation of a significant impact on the global distribution of economic, military, and political power (*Ibid.,* p. 172). Overall, one key point of the two scholars is that an accurate comprehension of the synergy between AI and national and global security is "far from being straightforward."(*Ibid*., p. 171)

Burton and Soare (2019) maintain that the scholarly works approaching the link between AI and security can be split into two schools of thought. The first one is focused on the revolutionary impact of AI deployment in security and defense. By the revolutionary impact of AI is meant the "effect on operations, capabilities and military structures and on how militaries interact with the civilian and political realms."(Burton & Soare, 2019, p. 3) A group of authors that belong to this school of thought include the names Johnson, Garcia or Daricili. Johnson argued in his paper that the military-use of AI is fast

becoming a major source of instability and great power strategic competition (Johnson, 2019, p. 150). Through his study, Johnson unraveled three key findings. First, the swift and inexorable proliferation of AI weapons has the potential to generate an international security crisis, nuclear-level warfare being the most significant concern (*Ibid*.). Second, the line between physical and digital security is gradually more blurry (*Ibid*., p. 160). Therefore, "the scope and scale" of future cyber-attacks will inevitably expand, which causes further intricacies in defense planning and strategic forecasting (*Ibid.*). Lastly, the new and fast emerging 'arms race' between the US and China "to innovate in AI will have profound and potentially highly destabilizing implications for future strategic stability." (*Ibid.*) of the international system.

Following the same narrative, but from a law perspective, Garcia argued in her analytical essay that the volatility of the international system caused by the militarization of AI can be solved by adopting "preventive security governance frameworks grounded on the precautionary principle of international law." (Garcia, 2018; Garcia, 2016) Her scrutiny focuses on how the three domains of peace and security as enunciated by O'Connell (2008) will be disrupted by lethal AI weapons. While recognizing that AI technologies brought about innovations in the military field, the focus of Daricili's analysis is on the challenges that, he asserts, "have not been experienced before in terms of global power struggle of states." (Daricili, 2020, p. 52) To display his argument, he carried out a comparison of the military objectives related to AI of the US, People's Republic of China and the Russian Federation. His outcome emphasizes that the battle for innovation of AI is currently fought between the US and China, with the Russian Federation following closely behind the two (*Ibid.*, p. 65). The ending remark of Daricili is that presently, the global AI sector serving military purposes is dominated by these three states.

The second school of thought maintains that "AI will have a more evolutionary impact, [...], that its focus will be on increasing the efficiency of [...] military tasks and on the speed of decision-making [...] without

fundamentally changing the nature of warfare." (Burton & Soare, p. 3) Authors such as Singh Gill, Masakowski, and Kechedji wrote academic studies that endorse, to a certain extent, the argument of this school of thought. Throughout her research, Masakowski took a comprehensive approach to the implications of AI. In this regard, she claims that "AI technologies will provide a means for safeguarding a stable environment in which the national security strategy, productivity and economic progress is ensured." (Masakowski, 2020, p. 3) In the military field she contends that, at a national level, new strategic pathways for national security strategies are possible due to the advancements in AI technologies (*Ibid*.). Hence, the new technologies are serving "as a force multiplier in support of" both a nation's strategic objective and decision-making capabilities (*Ibid*., p. 15). At a global level, preserving security and shaping a better future will be possible if leaders are committed to develop a common understanding of AI technologies (*Ibid.*, p.10).

Much like the previous authors, Singh Gill argued in her article that AI will reshape the nature of warfare, develop new capabilities and shift the balance of power in the international system (Gill, 2019, p. 169). An interesting observation that she makes is the non-recognition of the existence of lethal autonomous weapons by states (*Ibid.*, p. 175). Such a situation creates distrust, thus an impediment to building effective systems to regulate AI, especially in the military field (*Ibid*.). The way forward, she claims, is the governance of AI based on three factors: "a correct understanding of the power and limits of the technology, [...] a tiered approach" that includes actors from all sides of the spectrum, and trust and confidence between the states (*Ibid.*). Upholding the arguments elaborated by the previous researchers, Kechedji et al. made an interesting point, that for the proper use and implementation of AI (not only in the military field), governments need to invest in better education and training in AI (Tilovska-Kechedji & Bojovio, 2018, p. 10). The authors are also arguing that irrespective of the advantages of AI, the technology "should not be left autonomous to decide on issues which are crucial for the human being." (*Ibid.*,

p. 16)

Conclusively, in the security realm (understood from a realist perspective) the consensus among authors is that AI will have a tremendous effect. The rearrangement of the international system and the ongoing evolution of autonomous weapons are among the primary concerns found in the literature on this topic. Most of the scholars acknowledged the revolutionary effect of AI on military capabilities that is conducive to a new 'arms race'. As such, crucial issues namely the rapid proliferation of AI-enabled weapons, the high number of investments, and the more prevalent willingness to use lethal autonomous weapons in combat account for the concerns listed by academicians in their work. The others have conducted their research from a vantage point, claiming that the multitude of strategic benefits that AI can bring forward outweighs the disadvantages. However, and especially in the military field, the technology should be carefully treated and tailored to obey ethical norms and principles and should never be left without human-sight.

1.2.3 Artificial Intelligence (AI) in the European Union sphere

In the EU, the topic of AI was firstly approached by the European Parliament in 2017. The institution released a Resolution on the Civil Law Rules on Robotics. Since then, the implications of AI in the EU were thoroughly researched by experts in the domain and policymakers alike. Five years later, a plethora of official documents on the topic was published by the most relevant EU institutions such as the European Commission (EC) or the European Parliament (EP). Despite the obvious progress and efforts of integrating the new technology into the EU space, the area received relatively scant attention from scholars. There are, however, a handful of authors who focused their research on the approach of the EU over AI. The discussions are mainly centered around the integration stage of the new technology into the Union or the potential implications of AI in various sectors, from economy to defense. In her research, Inga Ulnicane examined how the EU developed its AI policies, and how it

positions itself regarding other global actors (Ulnicane, 2022, p. 255). Her outcome revealed that the EU, firstly, wants to distinguish itself from the main powers (the US and China), through its human-centric and ethical-based approach to AI (*Ibid.*, p. 265). Secondly, due to the limited competencies that the EU has in the military/defense area, discussions about "potential developments towards Military Power Europe based on AI investments" are fairly limited (*Ibid*.).

In their policy briefs, Boulanin et. al along with Fiott and Lindstrom assessed more concretely the military and defense implications of AI in the EU. In 2018, "the implications of AI for EU security and defense were largely unknown […]", with "potential unintended legal, ethical and operational consequences […]" (Fiott & Lindstrom, 2018, p. 1). Therefore, Fiott and Lindstrom recommended ways in which AI can be safely used for the enhancement of, first and foremost, the Common Foreign and Security Policy (CFSP), then other capabilities such as situational awareness, analytical tools, training of military personnel, etc. (*Ibid.*, p. 7). Two years later, Boulanin et. al argued that the EU has limited competencies in the field of armament and arms control (Boulanin et. al, 2020, p. 2). However, the discussion of responsible military use of AI in the EU is relevant specifically because of the EU's ambition of achieving strategic autonomy (*Ibid.*, p. 3). From this standpoint, the authors emphasized the role of other institutions and projects, such as the European Defense Agency (EDA) and Permanent Structured Cooperation (PESCO), in fostering AI in the military/defense sector of the EU (*Ibid*.). In the key findings section, the scholars have claimed that the groundwork of a "European view on responsible use of AI, has already been laid." (*Ibid.,* p. 18) The efforts of the EC, EP, EDA and Member States are indicative of this groundwork. However, considerable work is still needed for the integration of AI in the military domain, to ensure that all the safety, legal and ethical requirements are met (*Ibid.*).

Overall, the discussions of the use of AI in the EU are mainly focused

on three general components: the current level of development of AI policies in the Union and its position in relation to other global powers; the particularities of EU's AI policies and the diverse implications of the new technology. Most of the concerns related to AI in the EU are of economic, social, or political nature (Caradaica, 2020; Efthymiou et. al. 2020; Ulnicane, 2022). There is, however, a growing interest in the implications of AI over the military/defense sector of the EU, having also different focuses such as autonomous weapons or cybersecurity (Fiott & Lindstrom, 2018; Boulanin et. al, 2020; Andraško et al. 2021; Nadibaidze, 2022).

1.3 Gaps and contributions

This section starts with a summary of the scholarly works outlined above, on the topic of Artificial Intelligence (AI) in Politics. The author introduces, afterward, the gaps and the consequent contributions of this research. As mentioned at the beginning of this chapter, the application of AI in politics is a comprehensive subject, which encompasses several sub-branches. Therefore, the present literature review is not intended to be all-encompassing or exhaustive on the topic. Rather, the appraisal of the academic references follows the research streams that are in line with the Research Question of this paper. Consequently, the secondary resources were organized into three distinct categories. First, the largest number of studies included in this literature review address the topic of governance of AI. From this standpoint, the main concerns addressed by the authors relate to the alignment of AI policies with morals and ethical values such as *transparency*, *accountability*, and *responsibility*; the system build-up of the new technology; the insurance of a holistic approach, that includes the interests and objectives related to AI of state actors, stakeholders, and the research community. The approaches to examining the topic vary from one author to another, however, the bottom-line argument of the researchers is that the governance of AI is a laborious endeavor. Therefore, the task of effectively regulating a technology that has no benchmark to measure

against represents both a challenge and a risk.

The second category addresses the implications of AI in security. The term 'security' is understood in realist terms by most authors. Therefore, the main implications of AI in security are reflected in the military/defense field or the change of dynamics in the international system. A handful of authors maintain that AI will help in the enhancement of weapons (more specifically lethal autonomous weapons), decision-making capabilities and development of the techniques and gadgets used by the intelligence services. More generally, the technology is perceived as a tool that can maximize tremendously the potential of military capabilities and the current rivalry in this sense is "fought" between the US and China. In turn, the new 'arms race' between the two great powers can shift the current dynamics of the international system. Ultimately, the last category looks at the contributions that focus on the influence of AI over the EU. Given the unique structure of the Union and the principles and values upon which it functions, the way in which AI is treated is rather unique from the rest of the global powers. As such, the human-centric approach to AI developed by the EU is prevalent in academic works. The efforts to create the approach were prompted by the drive of the EU to be original and not fall behind the current leaders in the domain (China and the US). A rather scant attention was given to the implications of AI for the security of the EU. However, the insights from the literature on this topic showcase the limited competencies of the EU in the military realm, hence the focus on matters of economic or social concern.

Having laid out the most relevant academic references that are fitting for this research, some gaps can be identified. First, the EU has a unique and complex structure of governance. Two of the most relevant institutions that constitute this structure are the European Commission (EC) and the European Parliament (EP). Given that both institutions have different attributions and responsibilities, an alignment is essential for the regulation of the new technology. The current studies analyze how AI is reflected in the EU by

looking mainly at the documents released by the EC. Yet, no study so far evaluated how other institutions, such as the Parliament, frame AI policies. Second, as 'security' is one of the main pillars for the stability of the Union, AI will inevitably play a crucial role in this sense. Currently, no study assesses how the EU institutions frame AI policies from a security perspective other than the military. Third, no academic work assesses whether the institutions are aligned in the delivery of AI security policies. Therefore, to fill in these gaps, the present study displays how the EC and the EP frame AI security policies. The author uses a unique model of analysis that allows for the construction of frames. The outcome illustrates that each institution frames AI policies through the lenses of different security sectors. Therefore, 'security' is perceived from more angles other than the military. Subsequently, the research analyzes the frames from a comparative perspective. The empirical qualitative analysis displays the differences and similarities in how AI security policies are framed between the two institutions. As such, initial implications for regulating AI can also be drawn from the comparison. Lastly, this research contributes to the broader study of the concept of AI governance. The originality is that, unlike other scholarly works, this dissertation looks at the governance of AI from a security perspective, which has not been reproduced before, having the main area of interest the EU. The study can also contribute to answering broader research questions. For example, the study can give insights on the shared views on AI of the Member States. The findings of the research can also be treated as a reflection of what the governance of AI looks like at a national level. As emphasized at the beginning of the chapter, the contributions of this research are needed for a better understanding of AI's applicability in politics.

Chapter 2. Theory and Research Design

Chapter 2, of this paper delineates the conceptual framework and the methodology employed for the case study of this research. As such, the chapter is structured as follows. **The analytical framework and conceptualization** section starts with the relevance of the chosen conceptual framework for this research. It then proceeds to conceptualize the term *Artificial Intelligence* (AI) and the general *Framing theory*. The section concludes with the *Policy framing* approach, following the scholarly work of Rein and Schon, titled "*Frame-Critical Policy and Frame-Reflective Policy Practice*" (1996). Significant for this research is what the authors call 'rhetorical frames'. The **operationalization** section then outlines how the concept is applied to the case study, drawing three hypotheses. Finally, in the **Research Design section**, the author outlines the model of analysis used to assess the case study of this paper.

2.1 Analytical framework and conceptualization

The Research Question of this paper is "*To what extent are there differences between EU institutions in the framing of Artificial Intelligence security policies?"* The case study focuses, first, on the construction of frames for the European Commission (EC) and the European Parliament (EP), based on their official documents. Second, the author analyzes the frames from a comparative perspective, to determine the similarities and differences between the institutions. Consequently, for an accurate representation of the case study at hand, the *Framing* theory was selected to serve as a conceptual framework. Frames are "essentially used to provide meaning" (Olsson & Ihlen, 2018, p. 1). In the context of this research, *Framing* represents an adequate analytical model for three reasons. First, the *Framing* theory has a wide applicability across a variety of "academic disciplines such as sociology, political science, media studies, and strategic communication" (*Ibid.*). Given its versatility, *Framing* theory can be easily adapted to any research, to demonstrate how an issue is

rendered, who are the actors involved, and how the subsequent framing can affect the course of action in the future. Second, the multidisciplinary feature of the *Framing* theory prompted scholars to develop a myriad of frame patterns. Various models for constructing the frames are currently available. However, while following a certain frame gives the researcher a sense of direction and criteria to follow, it does not impede them to develop a new frame(s), based on the findings of the study (see Ulnicane et al., 2022; Ulnicane et al., 2021). Of relevance for this research is the *policy framing* approach developed by Rein and Schon. In short, Rein and Schon argue that policy frames are "diagnostic/prescriptive stories that tell, within a given issue terrain, what needs fixing and how it might be fixed" (Rein & Schön, 1996, p. 89). Lastly, the theory endorses the originality of this research. Researchers do not usually apply *framing theory* for the assessment of policies. The theory is even more rarely used to understand the interplay between new technologies and security policies. Therefore, this research brings a new approach to the concept of *Framing* and upholds its versatility.

2.1.1 Artificial Intelligence

To this day, there is no unanimously accepted definition for Artificial Intelligence (AI) among experts, scholars, and decision-makers alike. Nonetheless, such a context enabled policymakers around the world to create their approach to AI, tailored to their interests and objectives. In the European space, AI came into the limelight in early 2017, when the European Parliament (EP) adopted its resolution on *Civil Law Rules for Robotics* (European Parliament, 2017). Despite being the first EU policy document that referred to AI, it does not include a definition of the new technology. It wasn't until April 2018, when the European Commission (EC) released a Communication entitled *"Artificial Intelligence for Europe"*, that the new technology was defined (European Commission, 2018a). The definition goes as follows:

"*Artificial Intelligence refers to systems that display intelligent behavior by analyzing their environment and taking actions - with some degree of autonomy- to achieve specific goals. AI-based systems can be purely software based acting in the virtual world [...] or AI can be embedded in hardware devices [...].*"

(European Commission, 2018a, p. 1)

The subsequent documents that followed EC's Communication either remained consistent with the definition or broadened its scope. Regardless of the variations in the EU policy documents, defining and framing AI are two distinct elements. Hence, the following section introduces the *Framing* theory.

2.1.2 Framing theory

Taken broadly, the *Framing* theory -or in short *Framing*- is "the process by which people develop a particular conceptualization of an issue or reorient their thinking about an issue."(Chong & Druckman, 2007, p. 105) The premise is, therefore, that an issue can be viewed from multiple angles, having different implications for different reasons. Nevertheless, and as Scheufele & Tewksbury (2007) argued, *Framing* does not have an agreed-upon definition due to its applicability across numerous academic disciplines. Due to a strong correlation between media studies and political science, of particular prominence was the assessment of the *Framing* process's impact on how politics are communicated. However, few scholars attempted to use *Framing* as a means to understand how policies are constructed. One of the few scholarly works that approached the *Framing* process from this angle is "*Frame-Critical Policy Analysis and Frame-Reflective Policy Practice*" (1996), by Rein and Schon. Given that the case study of this research will focus on an assessment of how EU institutions frame AI security policies, the contribution of Rein and Schon is considered the most suitable model of analysis. Hence, the framework is further elaborated below.

2.1.3 Policy framing approach

Rein and Schon argue that generally a frame can be conceptualized in four different ways, one of them being "a generic diagnostic/ prescriptive story." (Rein & Schön, 1996, p. 88) The notion served as the foundation for the model of analysis constructed by authors who refer to frames "as strong generic narratives that guide both analysis and action in practical situations." (*Ibid.*) There are mainly two advantages of treating frames as generic narratives. First, they offer the possibility of having an integrative assessment of a policy issue (*Ibid.*). Second, narrative frames have a flexible nature in that they can accommodate changes easily (*Ibid.*). Moreover, the authors also suggested that frame narratives incorporate typically two notable elements: "framing devices" and "reasoning devices" (*Ibid.*, p. 89). These elements were identified by William Gamson (1983), who argued that, on the one hand, the "framing devices" are suggestive of how actors are thinking about an issue. On the other hand, the "reasoning devices" are a reflection of how the actors think they should approach the issue. These elements can take all sorts of forms, ranging from metaphors to icons or other symbolic devices, that can help the analyst construct "the core package" of a frame-narrative (*Ibid*.).

The elements outlined above are not, however, necessarily indicative of the existence of a frame. In the words of Rein and Schon, "frames are not self-evident." (Rein & Schön, 1996, p. 90) For the construction of a frame, there needs to be some sort of evidence that can guide the researcher in their appraisal. Therefore, Rein and Schon based the construction of their frames on two different contexts of policy discourse, specifically because frames are treated as generic-narratives. The first context looks at the policy debate, whereas the second is focused on the level of action in the implementation of policies. The frames belonging to the first context are referred to as 'rhetorical frames' and the ones belonging to the second as 'action frames' (*Ibid.*). Of particular relevance for this research are the 'rhetorical frames', due to their emergence from the 'policy-relevant texts' (*Ibid.*). In this case, there are three key elements

that a researcher should look for in the text: coherence, persuasiveness, and obviousness (*Ibid.*). The authors did not outline specifically what is meant by the three terms, which represents a challenge for the present dissertation.

Conclusively, the authors drew attention to a key point that is pertinent to highlight here too. As noted above, the construction of frames is based on evidence that follows the three criteria. The evidence under scrutiny requires the interpretation of the analyst over certain aspects, such as beliefs, meanings, and implications of the action. Therefore, the three criteria outlined above are defined by the analyst conducting the research. There is a possibility of encountering a certain degree of ambiguity "because the same beliefs and meanings can be consistent with different courses of action and attitudes toward truth" (*Ibid.*, p. 90).

2.2 Operationalization

The case study of this research is centered on how the EP and the EC frame AI regarding security, as mirrored in their official documents. Subsequent to the construction of frames is a comparative analysis that can depict the similarities and differences between the two institutions. Since 2017, regulating AI has become one of the top priorities on the agenda of EU policymakers. Regulating the new technology entails, among others, several effects on the security of the Union. These effects can be perceived discordantly if there are differences in how 'security' is conceptualized at the level of the institutions. Both the EC and the EP released documents that evaluate the potential impacts of AI on the security of the EU. Hence, to efficiently answer the Research Question of this paper, the *Policy Framing* approach developed by Rein and Schon is employed. More specifically, the paper engages with the model for 'rhetorical frames', that are shaped by the evidence from the "policy-relevant texts" (Rein & Schön, 1996, p. 90) as explained in the previous section.

In constructing the 'rhetorical frames', the analyst should look for three key aspects in the text: coherence, persuasiveness, and obviousness. The texts

selected for this research are gauged against this set of criteria which requires the interpretation of the author of this research. 'Coherence' is rendered as the quality of being systematic and logical (*Definition of COHERENCE*, n.d.). The texts should, therefore, have an integrative approach, following a clear line of argument(s). 'Obviousness' is defined as the quality of being easily seen and/or understood (*Definition of OBVIOUSNESS*, n.d.). The benefits, issues, and solutions brought about by AI for the security of the Union should be evident. 'Persuasiveness' is commonly defined as the capacity to move by argument or course of action (*Definition of PERSUASIVENESS*, n.d). For this research, the term refers to the capacity of the text to convince the audience of what AI entails for security, based on the presented arguments.

As such, utilizing the criteria showcases how both institutions are framing AI concerning security. Through the construction of frames, the author also conducted an empirical qualitative analysis over the frames. The analysis determined three elements that are used as variables of comparison between the frames of the institutions. The elements are the following: definition of AI, definition of security, engagement with the security sectors. These elements were chosen because they best assess the interplay between AI and security in the EU. Against this backdrop, three alternative hypotheses can emerge. The first hypothesis asserts that there are no differences in how the EP and the EC frame AI security policies. In this situation, the three elements outlined above are consistent across the institutions. The second hypothesis claims that there are slight differences in framing AI security policies by the EP and the EC. In this scenario, the differences are not significant. Few nuances of arguments can be observed in either of the three elements, yet the institutions can still reach a common ground. The last hypothesis affirms there are clear divergences between the EP and the EC in how they frame AI security policies. The presented arguments are distinct which means that the institutions are not aligned in how they want to regulate AI security policies.

2.3 Research Design

The research design of this paper uses a combination of *Framing* and content analysis. *Framing* is used for the construction of frames, based on the three key aspects identified by Rein and Schon: coherence, persuasiveness, and obviousness. As such, the case study uses the *Policy Framing* approach over the most relevant official documents released by the European Parliament (EP) and the European Commission (EC) that address the link between Artificial Intelligence (AI) and the security of the Union. To properly document the case study at hand, the author of this research conducted a process of data collection for the relevant EU official documents. The process took place between November 2021 and May 2022, approximately five years after the release of the first document in which AI was mentioned in the EU. Therefore, the data collected includes documents issued throughout the time interval of 2017-2021. Covering four years allows for a thorough understanding of how the framing process developed in the EU sphere. As the term "EU official documents" is rather ambiguous, the author developed a set of criteria to generate the dataset for this research:

- The official document can be found on the official websites of the EU;
- The official document is published by either the European Parliament or the European Commission;
- The official document is crafted independently and not as a reaction/response to another document;
- Due to feasibility reasons, the official document needs to have an option written in the English language;

To obtain the most accurate results, keywords such as *Artificial Intelligence in the EU*, *security*, *impact,* and other terms were used. Other search methods included the snowballing effect of reading secondary literature which made references to the documents, researching who are the most significant actors working on the topic or following the policy debates of the EP. A total of 26 official documents were identified. On initial reading, there are already

some notable differences between the documents: the length and format, if the product was the result of an independent study group, or of consultation with multiple stakeholders, for example. Due to a limited word space, however, the dataset had to be reduced to a lower number of official documents. Consequently, a process of data reduction was undertaken, consistent with testing the three hypotheses. The hypotheses are the following:

1. There are no differences in how the European Parliament and the European Commission frame AI security policies;
2. There are slight differences in framing AI security policies by the European Parliament and the European Commission;
3. There are clear divergences between the European Parliament and the European Commission in how they frame AI security policies.

The data reduction process reduced the dataset to a total of ten official documents, released by both the EC and the EP. Moving forward, the three hypotheses are going to be tested based on the frames that emerge as a result of the combination of *Framing* and content analysis. Content analysis is a method used by researchers to identify meanings, understandings, or "effects of communication content" (Luo, 2019). One of the benefits of content analysis is that it can be both quantitative and qualitative. For this research, the type of content analysis used is qualitative. Employing a qualitative content analysis presents three principal advantages. First, the sources of information can be studied without the direct involvement of the participants, hence the author of this research is free of any external influence (*Ibid*.). Second, a good qualitative content analysis follows a systematized procedure that can be reproduced by other authors (*Ibid.*). Therefore, the results yielded by qualitative content analysis are, in the majority of the cases, of "high reliability" (*Ibid.*). Lastly, the present methodology is malleable, meaning that access to suitable resources can be done at any given time and regardless of the location (*Ibid*.).

The qualitative content analysis was conducted by, firstly, undertaking

a coding procedure of the dataset. The coding procedure was performed via ATLAS.ti, a software for qualitative data analysis. In general, there are two types of coding for content analysis: inductive and deductive. Typically, qualitative content analysis requires a combination of both types of coding. However, for this study, the overarching approach is inductive coding. Inductive coding entails the creation of a coding scheme based on the findings from the texts. While the coding system was constructed as the author proceeded with the readings, there are still some deductive elements that guided the analysis. In line with the Research Question of this paper, which is *To what extent are there differences between EU institutions framing of Artificial Intelligence security policies?*, the coding system showcases features of frames of each institution, the EP and the EC. Examples of deductive elements that were looked to construct the set of codes included, for example, the type of security referred to in the documents (e.g. economic, social, military, political), whether AI is perceived as a challenge or as a benefit, how AI will be used to enhance security, etc. After the process of coding was finalized, the text analysis commenced with an initial visualization of patterns in the data. To do this, ATLAS.ti allowed for the export of lists of quotations by code. Visualizing the patterns in data rendered back the most prominent features of how AI is framed regarding security. Looking through these features, along with the criteria for *Framing* allowed for the construction of frames for each institution.

To briefly recap, this paper draws on a combination between *Framing* and a qualitative content analysis of ten official documents released by the EP and the EC, to effectively answer the Research Question. The research design was conducted in three stages. First, a process of data collection was carried out, to gather the most relevant EU official documents. The initial search of data presented 26 suitable documents for the case study of this paper. Due to the limited available space for this research, the dataset needed to be reduced. Hence, the second step was represented by a data reduction, consistent with testing the three hypotheses of this paper. Lastly, the content analysis of the ten

documents started with a coding procedure. The author used a specialized software to code, namely ATLAS.ti. As the Research Question does not present a particular set of ideas to investigate in the text, the author utilized the inductive coding approach. After the coding process was finalized, the analysis was followed by the visualization of the quotations by code. Visualizing the quotations revealed some recurrent patterns that together with the criteria set by the *Policy Framing* approach accounted for the construction of frames for both the EP and the EC. The findings of the research design are displayed in the next section of this paper.

Chapter 3. Findings

3.1 Context

The past few years have recognized an increasing level of action directed towards regulating Artificial Intelligence (AI) in the EU space. Two of the most important institutions, the European Commission (EC) and the European Parliament (EP), released policies that, supposedly, ensure a smooth incorporation of the new technology across all sectors of the Union. The recognition of risks and challenges entailed to AI is also prevalent across policies. Such a context raises questions as to how two institutions frame the interplay between AI and security in their policies, which serves the purpose of this dissertation. The last chapter of this paper is set to bring forward the findings of the research and is divided into two main sections, *Framing* and *Analysis*. Based on the sources of data collected and in line with the Research Question of this paper, the *Framing* section illustrates how AI security policies are framed by both the EC and the EP, followed by a comparative analysis of the frames. The research design determines some general aspects about each institution's framing of AI security policies. Subsequent to the general aspects are the frames developed for each institution. Lastly, the comparison segment introduces the main argument of this paper, highlights the originality, and reveals the validity of this research. Ensuing the presentation of the research outcome is the *Discussion* section which begins with the *Implications*. This section highlights, firstly, the potential consequences of a misalignment between the two institutions. An example in this sense is reflected in the AI act proposal, issued by the Commission in April 2021. Secondly, the section introduces the significance of the findings, to evaluate how the contributions are adding up to the existing knowledge on the topic. From this perspective, the evaluation of the findings will also bring forward the novelties of the research for the theory and practice of governance of AI. The next section recognizes the potential research limitations and their mitigation. Lastly, the final subsection, which is called *Future Research Agenda*, outlines some prospects for a future

research agenda in the area of AI governance or AI security governance.

3.2 Framing

3.2.1. Framing of Artificial Intelligence security policies by the European Commission

The European Commission (EC) is one of the most important institutions of the European Union (EU), representing the executive power. As such, two of its main responsibilities are to draft and propose new legislation (policies) to the Parliament and the Council and, after passing the Ordinary Legislative Procedure (OLP)[1], to implement these policies at the Union level. Debates about regulating Artificial Intelligence (AI) were consolidated in the EC in April 2018, with the release of the Communication "Artificial Intelligence for Europe" (European Commission, 2018a). Since then, the new technology became one of the top priorities on the agenda of the EC policymakers, who strived to create and deliver a comprehensive yet unique set of policies to govern AI. Due to its unpredictable nature, however, the security aspect is inherent to the effects of AI. In this respect, the content analysis conducted over the six official documents reveals, firstly, some general aspects that are noteworthy. Essentially, whilst the term 'security' is mentioned or engaged with several times throughout the documents, there is no definition or conceptualization of the word. Only one document out of the six that were analyzed sought to clarify the term by specifying that "Security is mostly implicitly assumed and covered by terms like 'trustworthy', 'robust', 'reliable' or 'resilient'." (European Commission, 2020a, p. 3) Therefore, the interpretation of 'security' is up to the author of this paper. Moreover, the Commission provides a specific definition of AI, however, it does not necessarily engage with it across the documents. Hence, the provisions set by

[1] The OLP is the standard procedure for adoption legislation, that starts with a proposal from the Commission and consists up to three readings from the Parliament and the Council, which need to reach a common ground (European Parliament, n.d.-b)

the EC for AI are rather vague and hinder further a clear illustration of the interplay between security and AI. Lastly, the EC has competencies in the areas of military and defense. These are two pivotal spheres for the maintenance of the security of the Union. Yet, the EC addressed rather rarely AI from the perspective of these two areas, despite claiming that "AI can significantly contribute to the objectives of the EU Security Union strategy." (European Commission, 2021a, p. 3)

Alternatively, the research design of this study identified that the EC treats the link between AI and security through three keyframes:

1. Artificial Intelligence inference on Economic Security;
2. Artificial Intelligence Implications for Social Security;
3. The maintenance of Political Security through ethical Artificial Intelligence.

The frames are derived from using the criteria for evidence stated by Rein and Schon, which are coherence, persuasiveness, and obviousness. Moving forward, the paper explores each frame, following a chronological order of the documents, starting from 2018 and ending in 2021. As will be elaborated below, while each frame targets a different area of security, some elements are recurrent across all frames, such as 'safety of the AI design', 'liability', or 'human-centric approach'.

Frame 1: Artificial Intelligence inference on Economic Security

One key focus of the EC found throughout all the analyzed documents is the application of AI across the European economy. The EC recognizes the tremendous power of the advanced technology and stated that "The EU should be ahead in technological developments in AI and ensure they are swiftly taken up across its economy." (European Commission, 2018a, p. 5) Nonetheless, the discussion of AI uptake over the economy does not, ineluctably, happen from a security perspective. Therefore, for the purpose of the analysis, the concept of 'economic security' is conceptualized by the author of this paper. 'Economic

security' is, perhaps, one of the hardest to define given the vast realm of economic theories and objects of reference. Nonetheless, for this research 'economic security' is understood in liberal terms as the capacity of the state (in this case the Union) to ensure its welfare and to create "stable conditions in which states can compete mercilessly." (Buzan et al., 1998, p. 98))

The importance of introducing AI across all economic sectors stems from the goal of the EU to remain competitive at a global level (European Commission, 2018a, p. 4). Hence, when the EC issued the European Strategy for AI, one of the primary goals indicated in the document was to "Boost the EU's technological and industrial capacity and AI uptake across the economy, both by the private and public sectors. " (*Ibid.* p. 3) The same goal was perpetuated and expanded in the documents that followed after the Strategy. For example, the Commission determined that the "Progress in AI opens the door to new opportunities in areas such as [...], fintech, advanced manufacturing, space-based applications, smart power grids, sustainable circular and bio economy, improved detection and investigation of criminal activities (e.g. money laundering, tax fraud), [...], etc." (European Commission, 2018b, p. 3) Moreover, the Annex for the Coordinated Plan on AI from 2018 notes ambitiously that "AI will be the main driver of economic and productivity growth and will contribute to the sustainability and viability of the industrial base in Europe." (European Commission, 2018b, p. 1) The same goal is endorsed in the White Paper from 2020, reinforcing the point that the EU must champion AI development due to the "fierce global competition" (European Commission, 2020b, p. 1). Lastly, in the Communication released in 2021, the EC goes as far as to state that "AI and other digital technologies can contribute to a sustained post-COVID-19 recovery due to their potential for increasing productivity across all economic sectors, creating new markets and bringing tremendous opportunities for Europe's economic growth." (European Commission, 2021b, p. 3). The reliance on AI to ensure economic security is, therefore, strongly emphasized through these statements.

Nonetheless, the economic security of the Union can be severely hampered if the management of AI is not properly handled. The apparent plethora of benefits that AI can bring to the EU's economic sector is counterbalanced by several risks and challenges. Interestingly, the Commission does not make the risks and challenges necessarily evident. Rather, they become more visible through the provisions that the EC is illustrating for the achievement of the goal. Overall, the research design of this dissertation identified three relevant risks and challenges that are recurrent across the documents. Before showcasing each issue, there are two notable aspects. First, the list of risks and challenges is in no way intended to be exhaustive. Rather, the author chose the issues based on the evidence that helped in the construction of the frame. Second, some of the risks and challenges classify also in the realm of social and political security, which will be expanded in the following sections of this chapter.

It has been clear since 2018 that, in the EC's view, one of the biggest challenges is for the EU to remain competitive at a global level is to "[...] to ensure the take-up of AI technology across its economy. European industry cannot miss the train." (European Commission, 2018a, p. 4) To address this challenge, the Commission mentioned that "a joint effort by both public and private sectors are needed to gradually increase overall investments by 2020 and beyond, in line with the EU's economic weight and investments on other continents." (*Ibid.*, p. 6). The same provision is reiterated and expanded across all the documents that were analyzed for this research. Most of the EC's endeavors are focused on stepping up the investments in the development of AI. Closely interlinked, the Communication that sets the Coordinated Plan of Action from 2018 recognized another challenge: "[…] small companies (which) do not know how to apply AI to their business, AI startups do not find the resources and talent they need in Europe […]" (European Commission, 2018c, p. 1) The same point is endorsed in the Annex for the Coordinated Plan: "Industry, and in particular small and young companies, will need to be in a

position to be aware and able to integrate these technologies in new products, services and related production processes and technologies, including by upskilling and reskilling their workforce." (European Commission, 2018b, p. 3) From this perspective, one of the provisions given by the Commission is to "Accelerate AI take-up through Digital Innovation Hubs" (European Commission, 2018b, p. 10) In the 2020 White Paper, the EC expanded the preceding initiatives by launching a regulatory framework meant to achieve an 'ecosystem of excellence'. Among others, the 'ecosystem of excellence' is meant to "create the right incentives to accelerate the adoption of solutions based on AI, including by small and medium-sized enterprises (SMEs)." (European Commission, 2020b, p. 3)

Particular attention was also devoted to data availability, a prerequisite for the existence and development of AI. However, the EC recognized that the availability of data is conditioned by various factors such as compliance with the current European legislation, the safety, and trustworthiness of the AI design (that needs to be free of bias and discrimination), the quality of data or the vulnerability to cyberattacks, to name a few. Some of these risks do not relate only to economic security which reinforces how versatile and dangerous the new technology is. Maintaining the focus on the security of the European economy, however, there are two notable initiatives brought forward by the EC. On the one hand, to make large datasets available, the Commission launched the initiative of having a common European Data Space, "a seamless digital area with the scale that will enable the development of new products and services based on data." (European Commission, 2018b, p. 13). Later, the Commission emphasized that "the promotion of AI-driven innovation is closely linked to the implementation of the European Data Strategy, [...] since AI can only thrive when there is smooth access to data. Especially small and medium-sized enterprises will need fair access to data to make a broad uptake of AI in the EU economy possible." On the other hand, in the attempt to prevent the above-mentioned risks and to construct an "ecosystem based on trust", the EC

believes that “it should follow a risk-based approach.” (European Commission, 2020b, p. 17). In particular, there should be a clear criterion that determines whether AI’s applicability is high-risk or not. The Commission indicates “that a given AI application should generally be considered high-risk in light of what is at stake, considering whether both the sector and the intended use involve significant risks, in particular from the viewpoint of protection of safety, consumer rights, and fundamental rights.”(European Commission, 2020b, p. 17)

To conclude, the first frame of the EC highlights evidently that AI represents a powerful tool that can foster the economy of the Union. From this perspective, economic security can be ensured as there is a high degree of reliance on AI to elevate the economic sector and allow the EU to be a global leader in the innovation of the new technology. Nonetheless, a flawed management of AI can cause multiple risks and challenges. The Commission acknowledges these issues through the provision of initiatives that are meant to prevent the risks or challenges from materializing. Pertinent with economic security, the research design determined three risks and challenges. Noticeably, the issues identified are interdependent. If the EU would not step up its investments in AI, it would not be able to support SMEs in the uptake of the new technology. Equally important, if data is not readily available, the functionality of AI is put under the question mark, as data represents its primary resource. However, the accessibility to large data pools is constrained by several other factors, as depicted above. Overall, the Commission gives the impression that it’s on the right path to achieving success in bringing AI to the EU’s economy and therefore sustaining its security. The fulfillment of the provisions is, nonetheless, time-dependent, as well as the outcome. Given that the regulation AI is only in its incipient phase, placing too much reliance on it for ensuring the security of the Union’s economy can prove to be rather prejudicial.

Frame 2: Artificial Intelligence implications for Social Security

Since 2018, the EC has committed to developing a unique approach to AI which is, above anything, human- centric. Hence and closely related to the economic welfare of the Union is the prosperity and safety of the society. The Commission is dedicated to ensuring that "No one is left behind in the digital transformation. AI is changing the nature of work: jobs will be created, others will disappear, most will be transformed. Modernization of education, at all levels, should be a priority for governments. All Europeans should have every opportunity to acquire the skills they need. Talent should be nurtured, gender balance and diversity encouraged." (European Commission, 2018a, p. 2) However, the discussion extends beyond the challenges posed by AI for the labor market. It relates also to other matters of social security such as the physical integrity of the EU citizens or respect for fundamental human rights. Once again, what is understood through 'social security' is fairly ambiguous as the Commission does not clarify it in its official documents. Therefore, in the context of the current study, the concept of 'social security' is defined by the author of this research. Intrinsically related to 'economic security', most definitions of 'social security' relate to the protection of people from phenomena such as inequality or poverty, and the insurance of access to services of healthcare or education, for example (*Facts on Social Security*, 2001). For this paper, 'social security' is employed from the perspective of these matters. It also adds that 'social security' addresses issues related to the physical integrity of the citizens, public safety and the protection of fundamental human rights.

The EC was well aware that European society will need to be prepared for the introduction of AI in everyday life. Hence, the second key focus of the Commission is to "Prepare for socio-economic changes brought about by AI by encouraging the modernization of education and training systems, nurturing talent, anticipating changes in the labor market, supporting labor market transitions and adaptation of social protection systems." (European

Commission, 2018a, p. 3) On the one hand, the Commission recognized the challenges entailed to this goal. Along with the difficulty of "preparing the society as whole" (*Ibid.*, p. 11) for the new technology uptake, the EC noted two other challenges: "[...] focus efforts to help workers in jobs which are likely to be transformed or disappear due to automation, robotics and AI [...] (and) train more specialists in AI [...]" (*Ibid.*) The Commission also recognized that "While the exact quantification of AI's impact on jobs is difficult to determine at this stage, the need for action is clear." (*Ibid.*) Ergo, the new technology is framed from the outset as a potential threat to social security. On the other hand, the potential benefits brought about by AI for social security are also highlighted by the EC. The palette of benefits ranges from performing dangerous tasks and assisting doctors with diagnosis to support people with disabilities (*Ibid.*).

Several provisions were launched to support the goal set by the Commission and address the probable challenges. However, the apparent focus on the impact of the new technology on the labor market was enlarged in 2020. In the assessment of the AI security risks and opportunities, the Commission noted that "AI is pervasive and can have extensive application in public security and cyber security, if sufficiently large data sets are available." (European Commission, 2020a, p. 4) As a result, several issues can arise such as invasion of privacy through CCTV surveillance or image analysis (*Ibid.*, p. 6). The Commission also noted that "AI is applicable for finding specific patterns in large datasets, and augmenting data. It can be applied to forecasting, planning, and scheduling tasks, which are for example prerequisites for predictive policing." (*Ibid*., p. 6) These features of AI can help in the prevention or tackling of several issues such as organized crime, drug trafficking, or border control issues. However, as data is the primary resource of AI, questions about its quality and integrity are again under the loop. Furthermore, using the biometric data of individuals -for surveillance purposes for example- contravenes again with fundamental human rights such as data privacy or the right to private life.

Similar to the applicability of AI in the economic sector, the safety of the AI design is also relevant for the maintenance of social security. The Commission noted that the "Use of AI in traffic management will meet citizen needs by reducing the number of victims and traffic accidents, ensuring mobility through proper traffic management and providing better management of all the procedures associated with traffic management." (European Commission, 2020a, p. 8) In this instance, there are two interlinked and essential considerations: the algorithm that rules the AI system and the degree of autonomy of the AI system. If the algorithm is malicious and the system is given full autonomy, lots of people's lives will be put in danger. Taken altogether, the EC stated that "While AI can do much good, [...], it can also do harm. This harm might be both material (safety and health of individuals, including loss of life, damage to property) and immaterial (loss of privacy, limitations to the right of freedom of expression, human dignity, discrimination for instance in access to employment), and can relate to a wide variety of risks." (European Commission, 2020b, p. 10) The Commission proposed a regulatory framework that, "will also work in tandem with applicable product safety legislation and in particular the revision of the Machinery Directive, which addresses - among others – the safety risks of new technologies, including the risks emerging from human-robot collaboration, cyber risks with safety implications, and autonomous machines." (European Commission, 2021b, p. 2)

Conclusively, the second frame of the EC perceives the wide spectrum of benefits that AI has for European citizens, but it's much more cautious in its approach to the new technology. The risks and challenges range from whether people will suffer from job losses to questions of privacy and individual safety. Extensive research from the side of the Commission was placed into creating feasible provisions that would address these issues. Such an effort stems from the willingness of the Commission to develop a human-centric approach to AI that is unique in the world. 'Social security' is, therefore, given great significance, by recognizing both the advantages and disadvantages of

implementing the new technology at the level of the Union.

Frame 3: The maintenance of Political Security through ethical Artificial Intelligence

The economic welfare and the safety of the society would not be sustainable without a strong governance structure that people can trust. The insurance of political security is, therefore, essential. 'Political security' is a broad concept, employed differently from one researcher to another. It can encompass elements from the spheres of economic, social, or military security which enhances the interdependence existent between the sectors (Buzan et al., 1998, p. 141). The Commission does not conceptualize the term in its official documents. However, based on the content analysis conducted for this research, the author determined that 'political security' is perceived, in the AI context, as the protection of the central values and core principles that constitute the foundation of the Union. The EC stated that "the Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities." (European Commission, 2019, p. 2) Consequently, the Commission mentioned in 2018 that it must "Ensure an appropriate ethical and legal framework, based on the Union's values and in line with the Charter of Fundamental Rights of the EU. This includes forthcoming guidance on existing product liability rules, a detailed analysis of emerging challenges, and cooperation with stakeholders, through a European AI Alliance, for the development of AI ethics guidelines." (European Commission, 2018a, p. 3)

The emergence of such a framework will be dependent primarily on two key principles. As the Commission mentions: "one key principle will be 'ethics by design' whereby ethical and legal principles, on the basis of the General Data Protection Regulation, competition law compliance, absence of data bias are implemented since the beginning of the design process. When defining the operational requirements, it is also important to consider the interactions

between humans and AI systems. The Commission will explore how to introduce an "ethics by design" principle in relevant calls for proposals under the research program. Another key principle will be 'security by design"', whereby cybersecurity, the protection of victims, and the facilitation of law enforcement activities should be taken into account from the beginning of the design process."(European Commission, 2018b, p. 8) As such, the Commission tasked a High-Level Expert Group to develop the ethics guidelines for the so-called 'trustworthy AI'. Reinforcing once again the uniqueness of the European approach to AI, the EC also added that "The ambition is then to bring Europe's ethical approach to the global stage." (European Commission, 2018c, p. 8) The efforts of the High-Level Group established that there are three components necessary for the achievement of 'trustworthy AI': "(1) it should comply with the law, (2) it should fulfill ethical principles, and (3) it should be robust."(European Commission, 2019, p. 3)

Nonetheless, the risks and challenges to developing a 'trustworthy AI' are acknowledged by the EC by stating that "The Guidelines of the HLEG should provide a common ground for security research programs. Especially (but not exclusively), the requirements for non-discrimination, privacy, robustness, safety, and transparency should be the basis of trustworthy European AI applications in security. However, this is a challenging goal given the current systemic security weaknesses of AI." (European Commission, 2020a, p. 11) To provide some examples, the Commission mentions that "[...] Novel attacks are also expected that take advantage of an improved capacity to analyze human behaviors, moods, and beliefs based on collected data. These concerns are most significant with authoritarian regimes but may also undermine the ability of democracies to sustain truthful public debates." (*Ibid.*, p. 13) Therefore, citizen participation in formal democratic processes can be placed under the risk. The Cambridge Analytica scandal is the most prolific example in this sense, in which thousands of psychological profiles were created based on the private data of Facebook users (Confessore, 2018). The

profiles were used for targeted voting during the US elections from 2016 (*Ibid*.). Such an event did occur on European soil. However, if the technological advances in AI are not properly regulated, they can transform into means to manipulate the masses. The threat directly undermines the political security of the Union. When it comes to the 'security of design', the EC mentioned that "the focus on ML (Machine Learning) has been at the expense of its security and the algorithms developed to enable it are not currently designed to prevent their malicious use. They are effectively insecure by design." (*Ibid.*, p. 5)

The significance of cybersecurity is also stressed by the EC, which mentions that "AI can be too vulnerable to targeted attacks if the attackers have direct access to the system and can feed it with spoofed or manipulated data. For example, researchers could fool a well-trained face recognition system with special crafted eyeglass frames and impersonate another person. Conversely, attackers can also apply AI to overwhelm classic security defenses or spoof digital media or evidence, which can also be hard to detect." (*Ibid.,* p. 6) The last example concerns the fairness and transparency of the decision-making process, a core component of any democratic society. The Commission mentioned that "Transparency of decision-making processes is a fundamental requirement in democratic societies. A usual requirement is the disclosure of the data categories used as input and the rules with which they are processed, at least on an abstract level. Currently, AI has not evolved sufficiently to provide a clear understanding of how decisions are arrived at. Especially in the case of false decisions ("false positives") by complex AI systems, it is currently impossible to understand the rationale for the erroneous decision." (*Ibid.*, p. 10)

To summarize, the last frame of the EC highlights the severe implications that AI has for the political security of the EU. The EC highlights that "opaque decision-making, gender-based or other kinds of discrimination, intrusion in our private lives or being used for criminal purposes." (European Commission, 2020b, p. 1) and even targeted voting are just a few of the threats and risks that can arise if AI is not properly regulated. Hence, safeguarding the

ethicality of the new technology plays a key role in addressing the potential sets of risks and challenges posed to political security. In this regard, the Commission tasked a High-Level Expert group to develop ethics guidelines for the creation of 'trustworthy AI'. The group determined seven key requirements for AI to be 'trustworthy' and, hence accepted in society. These requirements are, however, "non-binding and as such, do not create any new legal obligations" (European Commission, 2019, p. 3) From this perspective, the protection of the fundamental values and principles of the Union from the possible risks and challenges brought about by AI is still under the question mark.

3.2.2. Framing of Artificial Intelligence security policies by the European Parliament

The European Parliament (EP) represents one of the legislative bodies of the European Union (EU), along with the Council. Under the Ordinary Legislative Procedure (OLP*), one of the Parliament's main responsibilities is to debate, amend, adapt or reject EU legislation proposed by the Commission. Furthermore, due to its supervisory powers, the Parliament also has an indirect and non-binding influence on the EU's legislation, through non-binding resolutions and committee hearings. From this perspective, the Parliament is organized in standing committees, which are primarily designed to assist the European Commission (EC) in initiating legislation (European Parliament, n.d.-a). The discussions about Artificial Intelligence (AI) were consolidated in the Parliament- and in the EU for that matter- in 2017, when the Resolution on Civil Law Rules in Robotics was adopted (European Parliament, 2017). The Parliament was committed to the study of AI ever since and created a special committee dedicated only to the appraisal of the new technology. The Special Committee on Artificial Intelligence in a Digital Age (AIDA) was set up in June 2020. Its mission is to investigate the "impact and challenges of rolling out AI, identify common EU-wide objectives, and propose recommendations for the

best way forward." (Dragos Tudorache, 2020) Due to the limited space available, the content analysis was conducted only on three official documents of the EP. The reason is twofold. First, the official documents released by the EP are much lengthier and more detailed, in contrast with the ones released by the European Commission (EC). Second, the EP issues official documents at a higher frequency than the EC, given that the Special Committee works exclusively on AI. Hence, the official documents were selected in line with three factors: the most visited documents found on the EP official website on the topic of AI; equal distribution of documents across the chosen timeframe; the specificity of the content.

From this regard, the content analysis of this research reveals that the EP addresses the nexus between AI and security through two keyframes:

1. Artificial Intelligence and the impact on the civilian sphere;
1. Artificial Intelligence as a power that can enhance or threaten military security.

Same as for the EC, the frames were extracted by using the criteria for evidence stated by Rein and Schon, coherence, persuasiveness, and obviousness. Before diving into the scrutiny of each frame, there are some notable general aspects. The EP structures the discussion on AI through two streams: the current and the future opportunities and challenges presented by the new technology. The goal is to showcase why AI matters and why it should be treated with caution. On the one hand, AI presents great potential for the benefit of European society. The point is reinforced by the following statement: "The primary reason why AI matters is because of the immense potential it presents, both currently and speculatively, to benefit our lives." (Boucher, 2019, p. 1) On the other hand, the Parliament recognizes that AI exhibits also a vast array of challenges. The challenges are linked to the civilian and military spheres. Finally, whereas the EP stipulates what is understood by AI and engages with the definition of the new technology, it does a rather ambiguous job in conceptualizing the term 'security'. Hence, the word is down to the

interpretation of the author of this research.

Frame 1: Artificial Intelligence and the impact on the civilian sphere

In the civilian sphere, the challenges enumerated by the Parliament do not necessarily target just one area of security. Rather, the EP frames the discussions between AI and the security of the civilian sphere mostly through the current state-of-art of new technology. In its brief from 2019, the Parliament states the following: "[...] the same disruptions also present legal, social, ethical, and economic challenges. These are sometimes related to the technology itself, with questions of transparency, bias, and autonomy, or to the business models, which often prioritize gathering data or targeting advertising rather than delivering genuine social value." (Boucher, 2019, p. 1) Therefore, AI presents challenges for social, economic and political security altogether. In this context, 'security' is understood through the definitions provided for the frames of the European Commission (EC).

To begin with, the EP first indicates the transparency challenges related to AI. In total four challenges can make the new technology obscure. The first "and perhaps the most salient, is the lack of explainability of AI, that is, how the internal decision-making logic of an AI agent can be understood and described in human terms." (Boucher, 2020, p. 19) The Parliament claims that whilst the algorithm of an AI is constructed by a human, the way that the system performs its operations can be hard to pin down. The second challenge "is more deliberate, as some actors exploit imbalances in access to information to serve their commercial and strategic interests." (*Ibid.*, p. 20) "A third transparency challenge is that individuals do not always know whether they are interacting with an AI or human agent." (*Ibid.*) Lastly, "there is a longer-term challenge in the lack of transparency about the full range of intended and expected outcomes of AI development. Meaningful public debate and acceptance require transparency about the full range of expected impacts and uncertainties, both positive and negative. However, since the impacts are far from clear and there

remains a high level of uncertainty, it is not easy to provide this disclosure." (*Ibid*.) Taken together, these challenges can generate other risks and threats, as the paragraph below explains.

The current form of AI presents many threats such as disinformation, discrimination, and bias, as well as risks of value alignment, privacy, and data protection. In general, AI systems are not designed to be biased. However, some features, such as the quality of the data and the initial functioning mechanism of the AI algorithm, can make the new technology prone to prejudice and discrimination. To provide an example, the Parliament stated the following: "Consider a symbolic AI algorithm for examining job applications. It might evaluate candidates by assigning scores only on the basis of their education and experience. Yet, if it fails to take account of factors such as maternity leave or to appropriately recognize education in foreign institutions in ways that human selection committees would, the algorithm might discriminate against women and foreign candidates." (*Ibid.*, p. 22) To further accentuate the problem, even if the mechanism of the AI algorithm is altered, it still can retain information about how it previously operated. Hence, the algorithm can still be predisposed to bias, as the EP describes: "[...] AI algorithms cannot be objective because, just like people, in the course of their training they develop a way of making sense of what they have seen before and use this 'worldview' to categorize new situations with which they are presented." (*Ibid.*, p. 23)

The debate, therefore, extends to the values that will be perpetuated by the AI system and whether it can adapt to the changes happening in society. The Parliament argued that "[...] specific values such as privacy [...] can be deliberately embedded into the technologies 'by-design'." (*Ibid*.) However, "while today's AI development is rightly expected to respect contemporary perspectives on autonomy and privacy, these values could take a very different shape in the decades to come. If we develop too much lock-in, there is a risk that they will gradually become misaligned as society changes." (*Ibid*., p. 24) Moreover, the right to privacy (and other fundamental human rights) can also

be breached by accessing the personal data of individuals. One of AI's features, facial recognition, is representative in this sense. The EP contends that while the feature can be useful to identify missing people or suspects, for example, it can also be used for ill-intended purposes such as delivering tailored content to influence voters in political campaigns (*Ibid.*, p. 24-25). The data present on social media is also susceptible to usage by AI algorithms. In this respect, the Parliament claims that "The meaningful implementation of rules around informed consent is crucial to defend citizens from increasing categorization and control by both chillingly accurate and shockingly inaccurate algorithms." (*Ibid*.)

In describing how AI can influence the disinformation phenomenon, the EP gave the example of 'deepfakes'. The Parliament mentioned that "ML can be deployed to generate extremely realistic fake videos – as well as audio, text, and images – known as 'deepfakes'. The availability of data and algorithms make it increasingly easy and cheap to produce deepfakes, bringing them within reach of individuals with relatively modest skills and resources." (*Ibid.*, p. 21) Hence, together with dissemination platforms such as social media, "these applications present financial risks, reputational threats and challenges to the decision-making processes of individuals, organizations and the wider society." (Aengus, 2019) Besides, the socio-economic sector can also be impacted by AI through an uneven distribution of costs and benefits. The EP mentions that "the platform economy is one area where AI has already had a major impact on employment, with uneven distribution of costs and benefits, whereby a new generation of digital mediators facilitate transactions between producers and consumers." (*Ibid.*, p. 28) Competition between enterprises and organizations can, as well, be affected by the new technology. In describing the second transparency challenge, the EP claims that "ML can be used to analyze consumer data and predict individuals' 'willingness to pay' for items. Prices can be set at the upper end of the range and individual discounts sent to each shopper which – in effect – reduce the price to their estimated willingness to pay." (*Ibid*.,

p. 19) The practices can present challenges to competition as well, but the imbalance access to algorithms makes it a hard endeavor (*Ibid.*, p. 26)

To wrap it up, the first frame of the Parliament underlines the implications of AI for the security of the civilian sphere. In presenting the implications, the Parliament emphasizes the significant role of the technical design of AI. As such, the transparency challenges act as the start of a chain reaction for other threats and risks to the economic, social, and political security of the Union, as showcased in the paragraphs above. The EP acknowledges, though, that the new technology presents various opportunities that can be beneficial for European society, "such as supporting more effective health, production, transportation, and decision-making systems – as well as more frivolous benefits such as minor efficiency gains and novelty or entertainment value provided by a proliferation of 'gadgets'." (Boucher, 2019, p. 1) It even draws attention to the fact that the discussions on AI should not be focused on the challenges that AI exhibits. Rather, the debates should maintain a balance between the positive and negative implications, as the "Inadvertent underuse could result from failures to make the right strategic choices with regards to AI [...]" (*Ibid.*, p. 2)

Frame 2: Artificial Intelligence as a power that can enhance or threaten military security

The discussions about AI in the Parliament did not limit themselves to the impact of the new technology on the civilian sphere. Instead, the debate includes how AI unfolds in the military and defense realm. The EP argues that the new technology can bring both advantages and disadvantages to military security. For this research, 'military security' is understood in realist terms. As such, the state- in this case the Union- is the main referent object, which operates in a violent and anarchic system. Therefore, military power is essential to maintain the Union's sovereignty and defend itself from belligerence coming from external actors. Observed through this lens, the EP claims that the current

form of AI can shape the outlook of geopolitics and revolutionize the applications in the military and defense sector. Hitherto, the Parliament claims that the EU did not "engage in the power politics increasingly associated with AI." (Franke, 2021, p. 7) However, "even if Europe does not want to adopt the AI power politics narrative, or join the rhetoric about an AI race, it must consider the geopolitical implications of AI. It needs to consider the external dimension of its action, and how to deal with allies, partners, countries it wants to support, and opponents." (*Ibid.*, p. 8)

As it currently stands, the EU's conquest for securing a leading role in AI can be jeopardized due to a handful of factors. First, the Parliament contends that the EU worked throughout the years to augment its AI capabilities. However, a brief assessment of the Union's AI capabilities, development, and adoption showcases that "it lacks in certain areas and does not have a comfortable or secured lead in any of them." (*Ibid.*, p. 10-12) By contrast with other states, such as the United States (US) or China, the EU faces numerous challenges in expanding its AI capacities. These challenges range from a fragmented market to building an efficient AI system (*Ibid.*, p. 12) Second, the Sino-American competition for AI development already shapes the global balance of power. The new 'arms race' between the two states which presently possess tremendous amounts of AI capabilities, can inflict several challenges for the EU. One of the most significant challenges, the EP claims, is that the two spheres of influence will force the EU to eventually pick up sides, forcing a bandwagon effect (*Ibid.*, p. 16). Such a context places the Union in a delicate position, as both countries, the US and China, are relevant strategic partners for the continent. Moreover, "there is a concern that this competition could create dangerous incentives, such as fielding immature AI to gain an advantage over the competitor." (*Ibid*., p. 17)

Lastly, the new technology is largely privatized and governed by big tech firms. In this regard, the Parliament states that "The shift in power from the state to the private sector, and particularly to big tech firms could become

one the most fundamental changes in how politics functions in this century." (*Ibid.*, p. 19) Consequently, the management of AI by the private sector can raise numerous challenges. From a balance of power perspective, the EP mentions that "the state has less sway to influence the direction of research in a direction that is beneficial to it." (*Ibid.*, p. 20) In turn, big tech firms have more power to pursue their agenda (*Ibid.*), which can become extremely problematic. The military sector can also be heavily affected by the privatization of AI. One of the most crucial risks, the Parliament determines, is that the military can become a mere customer of the private sector, "rather than (being) in the driving seat of technological innovation." (*Ibid.*) In addition, tech companies are less inclined to work with the military due to "[...] economic or ethical reasons [...]" (*Ibid.*, p. 21). However, like any other technology, AI brought about a new "revolution in military affairs."

At the moment, the EP argues that whilst the discussions around AI in the military and defense realm are mostly related to lethal autonomous weapons, AI-enabled systems have a variety of applicabilities. The "AI [...] support in the military realm are manifold, reaching from logistics to autonomous weapons, cyber warfare, and disinformation. It includes offensive and defensive systems, frontline, and support systems. New weapon technology can impact the relative military strength of a country or alliance, and might require, for example, the reallocation of funds, the development and funding of new research and development strands, [...]" (*Ibid.*) The EP notes further that "AI is of interest for militaries as AI can improve (cost) efficiency, speed, stealth, may help to shield humans from danger or alleviate psychological and physical pressure, and can offer new military capabilities." (*Ibid.*, p. 22) Whilst the enhancement of military capacities by AI is of interest for strategists and policymakers around the world, the new technology can also produce pivotal changes. The EP notes that these changes can range from the creation of new war doctrine to how the new technology is going to be used in combat (*Ibid.*, p. 21-22). Moreover, given the unpredictable and uneven evolution of AI, accurate assessments of the

implications of AI on military systems are difficult to make. It's certain, however, that the management of the new technology will prove to be a tough endeavor for the EU. The Parliament notes that a particular challenge derives from "the impact of AI on military interoperability, the ability of allied militaries to work together." (*Ibid.*, p. 28) The EU is composed of 27 Member States, each having different logistical capabilities to enable AI in their defense systems. The interoperability problem is further accentuated by the compatibility of technologies at a Union level. Moreover, NATO also plays an important role, not only as a probable constituent that can induce the EU into the bandwagon effect mentioned earlier but also because of eventual technological gaps (*Ibid*.). In general, the Parliament contains that "so far, most Europeans have overlooked the area of military AI in a way that is not sustainable. Europe should engage with the use of AI in the military and defense realm to strengthen its defense capabilities and help to guarantee the safety and security of its citizens." (*Ibid.*, p. 38)

To conclude, the last frame of the Parliament highlights the opportunities and challenges represented by AI for the military security of the EU. Following the realist paradigm, the EP maintains that AI is a powerful tool that can heavily influence international geopolitics and boost military capabilities. Yet, the EU did not treat AI from this angle and its efforts to develop and expand its resources might be hampered as a result. The Parliament showcases how factors such as the new 'arms race' between the US and China for a leading role in AI, the privatization of the new technology and even the augmentation of military capabilities are risks that need to be urgently addressed and tackled further in the governance of AI. If the EU does not enter the 'power politics narrative' (*Ibid*., p. 7) and does not consider the external implications of its approach toward AI, the EU will not be able to compete for a leading role in the research and development of the new technology.

3.3 Analysis of the frames from a comparative perspective

Given the evidence outlined above, the scope of this section is to present the similarities and discrepancies existent between the European Commission (EC) and the European Parliament (EP). The comparison looks at three different elements: the definition of security, the definition of Artificial Intelligence (AI), and engagement with the security sectors. The elements were identified through an empirical qualitative analysis of the frames. The list of variables for comparison is not intended to be exhaustive, but rather to showcase the originality and validity of this dissertation. Furthermore, the analysis section is also intended to bring forward the answer to the Research Question of this paper and lay down the groundwork for future implications. For example, a potential mismatch between the two institutions is already reflected in the new proposal for a regulation that governs AI, issued by the Commission in April 2021. Lastly, the analysis section endorses further the contributions of this research for the theory and practice of the governance of AI.

The Research Question of this paper is *To what extent are there differences between the EU institutions in the framing of Artificial Intelligence security policies?* For an accurate answer to the question, this paper employed the *Policy Framing* approach developed by Rein and Schon, more specifically the model for the design of 'rhetorical frames'. Following the three key pieces of evidence for the construction of a 'rhetorical frame', persuasiveness, obviousness, and coherence, and based on the content analysis, the author managed to draw three frames for the EC and two for the EP respectively. The frames showcase that security is engaged through multiple sectors. These sectors are economy, social, politics and military. Therefore, this research demonstrates that taken altogether, the Commission and the Parliament have an all-inclusive approach to the interplay between AI and security. Nonetheless, there are some prominent similarities and differences between the two institutions.

Firstly, despite the clear evidence that indicates the link between AI and

security in the EU, none of the institutions define the term ‘security’ in their official documents. This is a recurrent practice of the EU, which sought to have an all-encompassing approach towards ‘security’ throughout the years. Yet, a proper definition of the term is still non-existent in the policy documents or strategies for security and can only be assumed. Several issues can arise as a result. For example, without a proper definition and engagement with the concept of ‘security’, the management of the new technology in this sense can be flawed. Given the volatile nature of AI, the lines of action need to be carefully tailored to also meet the requirements needed for the insurance and maintenance of what the ‘security’ of the Union stands for. However, if the term is not conceptualized plainly, the recognition of risks posed by AI and the delivery of provisions can lack substance. In addition, the EU rests upon a governance structure that represents the core of the Union. The absence of a proper conceptualization of the term ‘security’ can question the very essence of the Union. The gap does not only leave room for interpretation but also illustrates a misalignment between the institutions that constitute the governance structure.

Second, both institutions define what it is meant by AI. Nonetheless, the EC and the EP engage differently with the term. The frames display that whereas the EC rarely refers to the technical features of AI, the EP places a heavy emphasis on the state-of-art of the new technology. If the definition of AI is not sufficiently specific and does not have a common understanding across the institutions, then an effective governance of AI is implausible. Third, a similarity shared by the EC and EP is that they both frame AI as a tool for the progress of economic, social, and political security, but also as a threat. However, on the one hand, the EC’s approach is more centered on the provisions that exploit AI for the benefit of these three sectors. On the other hand, the EP is more invested in the display of the potential risks and challenges posed by AI. Such a dissimilarity points toward the different sets of interests and objectives of the two institutions. The Parliament has a preventive and

cautious approach to AI, considering its multi-faceted and risky nature. The Commission is proactive and sets lines of action without stressing the potential pitfalls of the new technology. Hence, the efficiency of the potential governance of AI can be easily hindered.

An additional difference in the engagement with security sectors that surfaced through the content analysis is that the EP engages with speculative opportunities and challenges of AI, which the EC does not. AI escaping human control, AI making employment obsolete, or the new technology developing its own "mind", are just a few examples acknowledged by the EP in the delivery of their policies (Boucher, 2020). Indeed, the debates about the potential development of Artificial General Intelligence (AGI) or Superintelligence (SI) are recurrent among scientists and researchers alike. That the EC does not make speculations concerning AI points, yet again, to a misalignment in vision, purpose, and action on behalf of the two institutions. Possibly the paramount similarity shared between the institutions is the emphasis on the role of data. Both the EC and the EP emphasized in their documents that one of the prerequisites for a proper functioning of AI is quality data. Indeed, data represents one of the three cornerstones -along with talent and computing power (Franke, 2021, p. 9)- that enable the avail of AI. Nonetheless, the availability of quality data is conditioned by several factors such as compliance with the current EU legislation or the safety and trustworthiness of the algorithm governing the AI system. Consequently, data acts as an impetus for most of the concerns related to AI in all three areas of security. At least from this perspective, there is a common ground between the two institutions. However, having just one crucial point of convergence is problematic.

Lastly, probably one of the greatest divergences between the Commission and the Parliament is that the EC does not frame AI from a military security perspective at all. Such a finding comes rather as a surprise as unlike the Parliament, the Commission has competencies in the area of defense and security. For example, the High Representative of the EU for Foreign Affairs

and Security Policy (HR/VP)- who is one of the vice-presidents of the EC- is responsible for the management of the Common Foreign and Security Policy (CFSP). The CFSP is arguably one of the most important instruments for the insurance of the security and defense of the Union. Moreover, the HR/VP announced in 2020 that one of the primary objectives of the EU is to gain 'strategic autonomy' (Borrell, 2020). The HR/ VP claimed that obtaining 'strategic autonomy' is more salient than ever as it is hard to be regarded as a 'global player' without having autonomy (*Ibid.*). More recently, the HR/ VP worked closely with the Council and adopted in March 2022 the Strategic Compass. The Strategic Compass is an eight year action plan, meant to "make the EU a stronger and more capable security provider." (Council of the European Union, 2022). Therefore, the fact that the EC does not frame AI from a military security perspective raises several concerns. First and as the EP argues in its study, AI is currently treated by other states, such as China and the US, as a geopolitical power that has the potential to shape future power dynamics. The unrecognition of this side of AI by the Commission will prompt the EU to pick one of the sides in the new 'arms race'. Such a context opposes the goal of obtaining 'strategic autonomy' and prevents the EU from ever championing the development and research of AI. Second, the EU was built and consolidated on values such as diplomacy, democracy, and multilateralism, which makes the Union a soft power. Nonetheless, the EU still developed military capacities throughout the years, to ensure that the defense and security of the Union do not solely rest on NATO. AI has, in its current form, several military applications. The EP pointed towards these applications that range from lethal autonomous weapon systems used in combat to cyber-operations. Even if the EU is not - and probably will never be a hard power-, the current security environment is fluid which requires the EC to consider AI's uptake in this sense too. Otherwise, the protection and security of the citizens and the EU per se can be put in jeopardy. Finally, the last concern points, once again, to the misalignment between two of the most important institutions of the EU. Perhaps

the most astonishing aspect is that whereas the EP has limited competencies in the area of security and defense, it still took more initiative and made a comprehensive analysis of AI's implications for military security. It is unclear why the EC does not frame AI in this regard. Nonetheless, it is still problematic given that the EU wants to be the first actor that develops a regulatory framework for AI.

To conclude, this section demonstrates that there are very few similarities and a lot of divergences between the EC and the EP. By looking at the three hypotheses delineated in the second chapter of this research, the closest one to answer the Research Question is the following: There are clear divergences between the EC and the EP in how they frame AI security policies. From this perspective, the insurance of proper governance of AI at the EU level seems highly unlikely. As stressed above, the uniqueness of the EU stands in the governance structure created by its main institutions. Despite the difference existent among the people ruling these institutions, a common ground should be always reached. In the case of AI, it seems that a consensus has not been achieved, and each institution pursues its agenda. The elements chosen for comparison are initial and are not reflective of all the similarities and differences existent between the EP and the EC. Instead, the comparison should be treated as an initial groundwork that can showcase the difficulties entailed in the governance of AI at a Union level. Moreover, the comparison can also be indicative of a larger phenomenon that circulates in academic circles that talk about a potential dismantlement of the EU.

3.4 Discussion

3.4.1 Research Implications and Contributions

The purpose of this section is to, first, highlight briefly how the outcome of this research is already reflected in the so-called Artificial Intelligence (AI) Act. Second, after depicting the present implications of the research, the author introduces possible future implications of the present outcome. Finally, the

section underlines the contributions brought forward to the existent scholarly works. In April 2021, the European Commission (EC) issued the Proposal on Laying Down Harmonized Rules for Artificial Intelligence (AI) (European Commission, 2021c). The policy document is the first one of its kind and is the result of four years of intense political deliberations. Supposedly, the regulatory framework should've been the outcome of both the Commission's efforts, and the work and recommendations of other actors such as the Parliament. It is out of the scope of this paper to provide an in-depth analysis of the document. Instead, a brief overview of the Act displays that much of the initial efforts of the EC are still focused on the economic and societal concerns of the increasing use of AI (*Ibid.*). One of the provisions even mentions that "AI systems exclusively developed or used for military purposes should be excluded from the scope of this Regulation [...]" (*Ibid.*, p. 20) Such an instance already endorses the argument of this paper which claims that there are clear divergences between how the European Commission (EC) and the European Parliament (EP) frame AI security policies. Whereas the EP was fairly vehement in the endorsement of AI implications for military security, the EC chose not to include it in the incipient phase of the regulatory framework. The present research does not engage with the consequent amendments that followed the release of the AI act due to space limit constraints. Nevertheless, the implications of a misalignment between the institutions are visible already in practice.

As for future consequences, one can argue that the misalignment between the EU institutions gives room for AI to become more rapidly a disruptive technology. The concept of 'disruptive technology' refers to the innovation that significantly alters the way in which consumers, businesses, or industries operate (Smith, 2022). It was already argued in this paper that AI has an uneven and unpredictable evolution. Hence, the technology needs to be carefully handled, and regulated especially in such a unique governance structure as the EU. Proper governance requires the main institutions of the EU

to be aligned. Unfavorably, currently there are a handful of divergences that can impede efficient regulation of AI to prevent it from becoming a disruptive technology. Moreover, the derangement existent between the EC and the EP also points towards a potential dismounting of the EU. Even if it's just in the context of regulating AI, the misalignment between institutions is indicative of a distrustful governance structure. As a result, Euroscepticism will rise among the EU citizens which is arguably one crucial element in the phenomenon of dismantling the EU. Moreover, speculations about the EU losing its strength and reaching an endpoint are already frequent both in policy and academia circles.

From an academic perspective, the novelties brought forward by this research are manifold. Principally, no study so far assesses how the EU institutions frame AI security policies. The body of literature lacks even more of an analysis that can illustrate whether there are differences between EU institutions in how they frame AI security policies. As such, the study contributes to both the governance concept and the *Framing* theory. The novelty in the case of governance is that this study analyzes it from a security perspective. In the case of the *Framing* theory, this research endorses its versatility. The empirical contribution of the dissertation stands in the display of frames for each institution and the subsequent comparison between them. The outcome of the unique research design employed for this research determined that the EC frames AI policies from the perspective of three security sectors, specifically economic, social, and political security. The EP frames AI policies from the same perspectives, but it also includes military security. One could argue that taken together, the Commission and the Parliament have an all-inclusive approach towards AI applications in security. Nonetheless, the comparison of frames depicts that the differences outweigh the similarities. In outlining both the divergences and similarities, the author was able to draw some initial consequences of a misalignment between the EC and the EP. Therefore, this dissertation argues that whilst the level of differences in framing

AI security policies between the EC and the EP cannot be quantitatively assessed, there are clear divergences between the two institutions. The research can be useful for the field of AI research and development, for the practice of an effective governance of AI and for the sensible implications of the new technology for security. The people that can benefit from this research range from specialists in the AI field, such as the ones that work for the Future of Life Institute, to EU policymakers, such as Commissioners, Members of the European Parliament or even Ministers of Foreign Affairs.

3.4.2 Limitations

The findings of this study must be seen in the light of some limitations. Among the most important constraints of this paper is the assessment of only a fair number of official documents. Due to the limited space, the author could not include more resources for the assessment of how the two institutions frame AI security policies. The inclusion of resources would've provided a clearer picture of the extent of differences between the EC and the EP. Here the author would also include that the research would have benefitted from an analysis of the AI act, and the consequent amendments delivered by the EP and the Council of the EU. Not including the work of the Council of the EU is another limitation. Apart from the limited space, the works of the Council are in general not publicly available, which would've also meant a scarcity of resources. Another limitation stems from model of analysis. The combination between *Policy Framing* approach and qualitative content analysis rests heavily on the author's interpretation of the criteria needed for the creation of 'rhetorical frames' and the texts from the policy documents. The empirical qualitative analysis rests also on the critical assessment of the author. As such, the model is prone to a certain degree of subjectivity which can affect the veracity of the findings. A further limitation includes the non-engagement with the effects of specific AI technologies, such as Machine Learning (ML) and Deep Learning (DL), over the security of the EU. These limitations do not shadow the accuracy of this

paper. The study has a clear research design and line of argument. Therefore, the findings brought forward have a solid basis, and as argued earlier, they constitute the groundwork for future research agenda.

3.4.3 Future research agenda

The last section of this chapter suggests future research directions. One course of action could investigate further the similarities and differences existent between the EC and EP. By using the findings of this research as a basis, a future study can also encompass the AI act in its assessment. It would be interesting to engage also with the Council's work on how it frames AI security policies. The institution represents an integral part of the governance structure of the EU. The spectrum of resources can also be enlarged to include, for example, media articles. Another interesting research stream would be the assessment of differences between the EU AI security policies and the National Strategies on AI developed by several Member States. Different logistical capacities have shown so far that very few Member States created their own National Strategies on AI. Hence, apart from the similarities and differences existing among the Member States, the level of interoperability of AI between the 27 Member States could also be explored. Potential new directions of study could also refer to the model of analysis used in this dissertation in contrast with other policymaking of either AI or another disruptive technology, such as the Internet of. Things (IoT). Lastly, the hypotheses of this research can be tested again in the future, to appraise whether eventually the institutions have reached a common ground or if the discrepancies are further accentuated.

Conclusions

The purpose of this dissertation was to determine the extent of differences between the European Commission (EC) and the European Parliament (EP) in how they frame Artificial Intelligence (AI) security policies. The study's outcome reveals that there are clear divergences between how the EC and the EP frame AI security policies. The argument of the paper was constructed following two lines of action. First, the study aimed to identify how two of the most important institutions of the EU, the EC and the EP, frame Artificial Intelligence (AI) security policies. For the construction of the frames, the author used a combination between the *Policy Framing* approach developed by Rein and Schon, more specifically the criteria for the construction of 'rhetorical frames', and qualitative content analysis. The outcome of the research design highlighted that the EC frames AI policies from the perspective of three security spheres, economic, social, and political. The EP's framing of AI policies happens from the same outlook of security, also adding the military security perspective. Second, by using the *Framing* theory, the author was able to determine three hypotheses. These hypotheses were investigated by analyzing the frames from a comparative perspective. The comparison was carried out against three elements: the definition of security, the definition of AI, engagement of the same sectors of security. Rather than following a premade model of comparison, the author conducted an empirical qualitative analysis over the frames to determine the comparative variables. As such, the elements for chosen as they can adequately depict the interplay between AI and security. The elements of comparison are not intended to be exhaustive or representative for all the similarities and differences existent between the two institutions. Regardless, the variables were sufficient to validate the third hypothesis, which claims that there are clear divergences between the EC and EP in how they frame AI security policies. Consequently, this dissertation argues that framing AI policies is distinctive at the level of the EU institutions.

The contribution of this study is manifold. The analysis determined how

the EC and the EP frame AI security policies, an outcome that has not been reproduced before. Moreover, the subsequent comparison of the frames rendered the similarities and differences between the EU's institutions, which no other study has attempted to do. Currently, the mismatch between the EC and the EP is reflected in the proposal for the AI Act, which was issued by the Commission in April 2021. This dissertation did not assess thoroughly the proposal, yet at first glance the provisions for the regulatory framework do not encompass many of the points endorsed by the Parliament. The comparison has also laid down the groundwork for future implications, such as the potential of AI to become a disruptive technology or even a dismount of the EU. Under the existing academic literature, the largest contribution of this dissertation falls under the governance category. The novelty brought forward is that no study so far assessed the governance of AI from a security perspective. The research also contributes to the concept of *Framing*, by upholding its versatility. The analysis can be also of use for specialists in the AI field or even policy makers working in the EU institutions. Nevertheless, this academic paper has not been eluded by limitations. The most striking stands in the research design of the paper, which rests heavily on the interpretation of the author. As such, the research is prone to a certain degree of subjectivity. However, the limitations do not eclipse the contributions, as the future research agenda is broad. Scholars can investigate further the similarities and differences between the EC and EP and include the official documents succeeding this research. The research can be extended to also include other institutions, such as the Council, or other sources including, for example, media releases. Potential directions could also refer to the research design of this paper in contrast with other AI or other disruptive technologies policymaking. That being said, the study holds a high relevance for both the academia and empirical studies.

Bibliography

Secondary Resources

Books

- Bevir, M. (2012). *Governance: A Very Short Introduction*. OUP Oxford.
- Borrás, S., & Edler, J. (2014). *The Governance of Socio-Technical Systems: Explaining Change*. Edward Elgar Publishing.
- Buzan, B., Waever, O., & Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.
- Jasanoff, S. (2016). *The Ethics of Invention: Technology and the Human Future*. W. W. Norton & Company.
- O'Connell, M. E. (2008). *The Power and Purpose of International Law: Insights from the Theory and Practice of Enforcement*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195368949.001.0001
- Rein, M., & Schön, D. (2002). Reframing Policy Discourse. In *Argument Turn Policy Anal Plan* (pp. 153–174). Routledge. https://doi.org/10.4324/9780203499467-8

Book Sections

- Alaca, A. İ. S. (2019). THE EFFECT OF ARTIFICIAL INTELLIGENCE TECHNOLOGY ON POLITICS AND INTERNATIONAL RELATIONS. In *Selected Discussion on Social Science Research* (pp. 782–811). Frontpage Publication.
- Masakowski, Y. R. (2020). Artificial Intelligence and the Future Global Security Environment. In Y. R. Masakowski (Ed.), *Artificial Intelligence and Global Security* (pp. 1–34). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78973-811-720201001

- Oke, S. A. (2008). *A Literature Review on Artificial Intelligence* (4th ed., Vol. 19, pp. 535–570). International journal of information and management sciences.
- Olsson, E., & Ihlen, Ø. (2018). Framing. In R. L. Heath & W. Johansen, The International Encyclopedia of Strategic Communication (1st ed., pp. 1–11). Wiley. https://doi.org/10.1002/9781119010722.iesc0076
- Ulnicane, I. (2022). Artificial intelligence in the European Union. In T. Hoerber, G. Weber, & I. Cabras, *The Routledge Handbook of European Integrations* (1st ed., pp. 254–269). Routledge. https://doi.org/10.4324/9780429262081-19
- Ulnicane, I., Knight, W., Leach, T., Stahl, B. C., & Wanjiku, W.-G. (2022). Governance of Artificial Intelligence. In M. Tinnirello, *The Global Politics of Artificial Intelligence* (1st ed., pp. 29–56). Chapman and Hall/CRC. https://doi.org/10.1201/9780429446726-2
- Vreese, C. H., & Lecheler, S. (2016). Framing Theory. In G. Mazzoleni (Ed.), *The International Encyclopedia of Political Communication* (1st ed., pp. 1–10). Wiley. https://doi.org/10.1002/9781118541555.wbiepc121

Journal Articles

- Andraško, J., Mesarčík, M., & Hamuľák, O. (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: Challenges and opportunities for the EU legal framework. *AI & SOCIETY*, *36*(2), 623–636. https://doi.org/10.1007/s00146-020-01125-5
- Ardam, S. M., Dehnavi, E. A., & Barzyan, M. G. (2021). SECURITY FROM THE PERSPECTIVES OF REALISM, COPENHAGEN, LIBERALISM WITH A LITTLE TASTE OF TECHNOLOGY. *PalArch's Journal of Archaeology of Egypt / Egyptology*, *18*(15), 636–658.

- Buiten, M. C. (2019). Towards Intelligent Regulation of Artificial Intelligence. *European Journal of Risk Regulation*, *10*(1), 41–59. https://doi.org/10.1017/err.2019.8
- Burton, J., & Soare, S. R. (2019). Understanding the Strategic Implications of the Weaponization of Artificial Intelligence. *2019 11th International Conference on Cyber Conflict (CyCon)*, 1–17. https://doi.org/10.23919/CYCON.2019.8756866
- Butcher, J., & Beridze, I. (2019). What is the State of Artificial Intelligence Governance Globally? *The RUSI Journal*, *164*(5–6), 88–96. https://doi.org/10.1080/03071847.2019.1694260
- Carabantes, M. (2020). Black-box artificial intelligence: An epistemological and critical analysis. *AI & SOCIETY*, *35*(2), 309–317. https://doi.org/10.1007/s00146-019-00888-w
- Caradaica, M. (2020). Artificial Intelligence and Inequality in the European Union. *Europolity*, *14*(1), 1–31.
- Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2017). Artificial Intelligence and the 'Good Society': The US, EU, and UK approach. *Science and Engineering Ethics*. https://doi.org/10.1007/s11948-017-9901-7
- Chong, D., & Druckman, J. N. (2007). Framing Theory. *Annual Review of Political Science*, *10*(1), 103–126. https://doi.org/10.1146/annurev.polisci.10.072805.103054
- Cummings, M. L., Roff, H. M., Cukier, K., Parakilas, J., & Bryce, H. (2018). *Artificial Intelligence and International Affairs: Disruption Anticipated*. Chatham House- The Royal Institute of International Affairs. https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf

- Daricili, A. B. (2020). The Impact Of Artificial Intelligence Management Upon International Security. *The Journal of Defense Sciences*, *19/1*(37), 24.
- Efthymiou, I.-P., Efthymiou -Egleton, T.-W., & Sidiropoulos, S. (2020). Artificial Intelligence (AI) in Politics: Should AI be controlled? *International Journal of Innovative Science and Research Technology*, *5*(2), 49–51.
- Fischer, S., & Wenger, A. (2021). Artificial Intelligence, Forward-Looking Governance and the Future of Security. *Swiss Political Science Review*, *27*(1), 170–179. https://doi.org/10.1111/spsr.12439
- Gahnberg, C. (2021). What rules? Framing the governance of artificial agency. *Policy and Society*, *40*(2), 194–210. https://doi.org/10.1080/14494035.2021.1929729
- Gamson, W. A., & Lasch, K. E. (1983). The political culture of social welfare policy. *Evaluating the Welfare State : Social and Political Perspectives*.
- Garcia, D. (2016). Future arms, technologies, and international law: Preventive security governance. *European Journal of International Security*, *1*(1), 94–111. https://doi.org/10.1017/eis.2015.7
- Garcia, D. (2018). Lethal Artificial Intelligence and Change: The Future of International Peace and Security. *International Studies Review*, *20*(2), 334–341. https://doi.org/10.1093/isr/viy029
- Gill, A. S. (2019). Artificial Intelligence and International Security: The Long View. *Ethics & International Affairs*, *33*(02), 169–179. https://doi.org/10.1017/S0892679419000145
- Goodman, B., & Flaxman, S. (2017). European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation." *AI Magazine*, *38*(3), 50–57. https://doi.org/10.1609/aimag.v38i3.2741

- Johnson, J. (2019). Artificial intelligence & future warfare: Implications for international security. *Defense & Security Analysis*, *35*(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800
- Kroll, J., Huey, J., Barocas, S., Felten, E., Reidenberg, J., Robinson, D., & Yu, H. (2017). Accountable Algorithms. *University of Pennsylvania Law Review*, *165*(3), 633.
- Lim, H. S. M., & Taeihagh, A. (2019). Algorithmic Decision-Making in AVs: Understanding Ethical and Technical Concerns for Smart Cities. *Sustainability*, *11*(20), 5791. https://doi.org/10.3390/su11205791
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 205395171667967. https://doi.org/10.1177/2053951716679679
- Nadibaidze, A. (2022). A Step Forward for the OSCE and European Security. *Geneva Center for Security Policy*, *22*, 12.
- Radu, R. (2021). Steering the governance of artificial intelligence: National strategies in perspective. *Policy and Society*, *40*(2), 178–193. https://doi.org/10.1080/14494035.2021.1929728
- Rein, M., & Schön, D. (1996). Frame-critical policy analysis and frame-reflective policy practice. *Knowledge and Policy*, *9*(1), 85–104. https://doi.org/10.1007/BF02832235
- Szpyra, R. (2014). Military Security within the Framework of Security Studies: Research Results. *Connections: The Quarterly Journal*, *13*(3), 59–82. https://doi.org/10.11610/Connections.13.3.04
- Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, *40*(2), 137–157. https://doi.org/10.1080/14494035.2021.1928377

- Tilovska-Kechedji, E., & Bojovio, M. K. (2018). Artificial Intelligence influencing foreign Policy and Security. *Journal of Eastern-European Criminal Law*, *2018*(2), 7–18.
- Ulnicane, I., Knight, W., Leach, T., Stahl, B. C., & Wanjiku, W.-G. (2021). Framing governance for a contested emerging technology:insights from AI policy. *Policy and Society*, *40*(2), 158–177. https://doi.org/10.1080/14494035.2020.1855800

Primary Resources

Official Documents

- Boucher, P. (2019). *Why artificial intelligence matters- Briefing European Parliament*. European Parliament.
- Boucher, P. (2020). *Artificial intelligence: How does it work, why does it matter, and what we can do about it?- Study Panel for the Future of Science and Technology*. European Parliament. https://data.europa.eu/doi/10.2861/44572
- DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIR. (2020). *AI AND SECURITY OPPORTUNITIES AND RISKS Towards a trustworthy AI based on European values PASAG report 3 - 2020 – AI and security*. European Commission.
- European Commission. (2018a). *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions—Artificial Intelligence for Europe COM(2018) 237 final*. European Commission.
- European Commission. (2018b). *ANNEX to the COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN*

ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Coordinated Plan on Artificial Intelligence COM(2018) 795 final. European Commission.

- European Commission. (2018c). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Coordinated Plan on Artificial Intelligence COM(2018) 795 Final*. European Commission.
- European Commission. (2019). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Building Trust in Human-Centric Artificial Intelligence COM(2019) 168 final*. European Commission.
- European Commission. (2020). *White Paper on Artificial Intelligence-A European approach to excellence and trust*. European Commission.
- European Commission. (2021a). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Fostering a European approach to Artificial Intelligence COM(2021) 205 final*. European Commission.
- European Commission. (2021b). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM(2021) 206 final*. European Commission.

- European Parliament. (2017). *Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)*. European Parliament.
- Franke, U. (2021). *Artificial Intelligence diplomacy | Artificial Intelligence governance as a new external policy tool- Study requested by the AIDA committee*. European Parliament.

Web pages

- *AI Winter: The Highs and Lows of Artificial Intelligence*. (2021, September 1). History of Data Science. https://www.historyofdatascience.com/ai-winter-the-highs-and-lows-of-artificial-intelligence/
- Borrell, J. (2020, December 3). *Why European strategic autonomy matters | EEAS Website*. EEAS - European External Action Service - European Commission. https://www.eeas.europa.eu/eeas/why-european-strategic-autonomy-matters_en
- Council of the European Union. (2022, March 21). *A Strategic Compass for a stronger EU security and defence in the next decade*. https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/
- *Definition of COHERENCE*. (n.d.). Merriam- Webster. Retrieved July 25, 2022, from https://www.merriam-webster.com/dictionary/coherence
- *Definition of OBVIOUSNESS*. (n.d.). Merriam- Webster. Retrieved July 25, 2022, from https://www.merriam-webster.com/dictionary/obviousness

- *Definition of PERSUASIVENESS*. (n.d.). Merriam- Webster. Retrieved July 25, 2022, from https://www.merriam-webster.com/dictionary/persuasiveness
- *Digital economy and society in the EU - What is the digital single market about?* (n.d.). [Eurostat]. Digital Technologies and in Particular the Internet Are Transforming Our World and the European Commission Wants to Make the EU's Single Market Fit for the Digital Age – Moving from 28 National Digital Markets to a Single One. Retrieved July 11, 2022, from http://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html
- Dragos Tudorache. (2020). *About | AIDA | Committees | European Parliament*. Committees European Parliament. https://www.europarl.europa.eu/committees/en/aida/about
- European Parliament. (n.d.-a). *Introduction | About | Committees | European Parliament*. Committees- European Parliament. Retrieved July 25, 2022, from https://www.europarl.europa.eu/committees/en/about/introduction
- European Parliament. (n.d.-b). *Overview | Ordinary legislative procedure | Ordinary Legislative Procedure | European Parliament*. European Parliament. Retrieved July 25, 2022, from https://www.europarl.europa.eu/olp/en/ordinary-legislative-procedure/overview
- European Parliament. (n.d.-c). *Powers and procedures*. Powers and Procedures. Retrieved July 15, 2022, from https://www.europarl.europa.eu/about-parliament/en/powers-and-procedures
- European Union. (n.d.). *Aims and values*. European Union. Retrieved July 14, 2022, from https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en

- Lewis, T. (2014, December 4). *A Brief History of Artificial Intelligence*. Livescience.Com. https://www.livescience.com/49007-history-of-artificial-intelligence.html
- Luo, A. (2019, July 18). *Content Analysis | A Step-by-Step Guide with Examples*. Scribbr. https://www.scribbr.com/methodology/content-analysis/
- Smith, T. (2022, April 2). *What Is Disruptive Technology?* Investopedia. https://www.investopedia.com/terms/d/disruptive-technology.asp

Policy Briefs/ Reports

- Boulanin, V., Goussac, N., Bruun, L., & Richards, L. (2020). *Responsible Military Use of Artificial Intelligence: Can the European Union Lead the Way in Developing Best Practice?* Stockholm International Peace Research Institute (SIPRI).
- Cummings, M. L., Roff, H. M., Cukier, K., Parakilas, J., & Bryce, H. (2018). *Artificial Intelligence and International Affairs: Disruption Anticipated*. Chatham House- The Royal Institute of International Affairs. https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf
- Fiott, D., & Lindstrom, G. (2018). *Artificial intelligence: What implications for EU security and defence?* European Union Institute for Security Studies (EUISS). https://data.europa.eu/doi/10.2815/689105
- Aengus, C. (2019). *Forged Authenticity: Governing Deepfake Risks*. Lausanne: EPFL International Risk Governance Sector. https://infoscience.epfl.ch/record/273296/files/IRGC%20Forged%20Authenticity%20Governing%20Deepfake%20Risks.pdf
- *Facts on Social Security*. (2001). International Labour Organization.

Media articles

- Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Interviews

- Dafoe, A. (2019). *GLOBAL POLITICS AND THE GOVERNANCE OF ARTIFICIAL INTELLIGENCE* [Journal of International Affairs].