Shuting Dai, *PhD Candidate*
School of Politics and International Relations, Tongji University.

Lilei Song, *Professor*
Deputy Director of Center for European Studies, School of Political Science and International Relations, Tongji University.
Email: songlilei@tongji.edu.cn

DOI: https://doi.org/10.37458/ssj.5.3.1
Research Paper
Received: September 14
Accepted: November 19

BALANCING SECURITY AND REGULATION: THE EU'S CONUNDRUM IN MILITARY AI GOVERNANCE

Abstract: *Artificial Intelligence (AI) has become an integral component within a wide array of weapon systems and critical infrastructure, serving as a fundamental framework for seamless integration with diverse technologies. However, the convergence of technology, military apparatus, and operational efficiency has facilitated the gradual securitization of technology regulation. This trend underscores the increasing portrayal of technology development as a matter of security relevance over recent decades. Facing a complex geopolitical landscape, the European Union's discussions on "strategic autonomy" and "technology sovereignty" encompass considerations of innovative advancements in defense technologies, particularly emphasizing the exploration of AI's potential for enhancing military security capacities. Meanwhile, regulation stands as a pivotal instrument within technology security policies, given AI's dual-use nature and its implications for geopolitical competition, the EU's ongoing efforts to establish comprehensive AI regulations are crucial. The regulation of more clandestine military AI applications remains a significant area of exploration for the EU. Consequently, the core research inquiry revolves around the EU's strategic alignment between security imperatives and regulatory frameworks concerning the military application of AI, aiming to ascertain its capability to strike a balance between fostering developmental capacities and implementing effective risk regulation.*

Keywords: *Artificial Intelligence; Military Security; the EU*

1. Introduction

The governance of military artificial intelligence (AI) is a key concern for scholars. A large number of studies on military AI have been placed in the research framework of national security. Scholars have focused on exploring how artificial intelligence affects national security, the subversion of the form of war, and other issues, arguing that artificial intelligence can redefine and change the development of military technology, bring about fundamental changes to military forces, and is an important field of strategic competition for major powers. At the same time, scholars have also proposed that the military AI has unpredictable and potentially highly destabilizing security implications and that the pursuit of technology and military superiority by some states may lead to an intensification of the arms race and mistrust, giving rise to new security threats, and exerting a far-reaching impact on the international security landscape. Some scholars have further analyzed the changes in weapons and combat modes brought about by military AI and have expressed their concerns about Lethal Autonomous Weapon Systems (LAWS) security threats.[1] In addition to researching the security implications of AI technology, scholars have also discussed, in ethical detail, the legal and governance paths of military AI.[2] The relevant research results present us with a more complete picture of the development of military AI, potential application space and risk concentration points, laying a solid foundation for the in-depth excavation of the relationship between AI and military security. However, there is still more space for military AI strategy at the regional and country level, and there is a lack of systematic analysis of the military AI policy tendency of the EU and its member states.

This article attempts to analyze the EU's institutional design, funding, and international participation in military AI and identify the EU's governance path towards military AI in the background of the geopolitical environment of increasing security threats and the pressure of the arms race of military AI. Based on relevant research, this paper will analyze and explore the potential security risks of military AI and then deconstruct in detail the EU's policy choices between the development of military AI capabilities and the regulation of security risks.

[1] See Johnson (2019); Geist & Lohn (2018); Horowitz (2018); Cave & ÓhÉigeartaigh (2017); Roff (2014); Horowitz (2019).
[2] See Scharre (2023); Anderson & Waxman (2017); Stix & Maas (n.d.); Schmitt (n.d.); Schiff et al. (2020); Stefan (2020)..

2. Military AI: potential and attendant risks

Military AI represents a transformative capability in the domain of security, offering unprecedented advancements in strategic decision-making, operational efficiency, and defense systems development. Applications such as autonomous platforms, AI-enhanced surveillance, and predictive analytics have the potential to significantly enhance the effectiveness of security frameworks. However, the inherently dual-use nature of AI, enabling its utilization across both civilian and military domains, introduces the proliferation of advanced capabilities to non-state actors. This duality provides a basis for examining the EU's approach to regulation and policy, as power in the normative domain is not only important for military AI governance, but also facilitates the establishment of dominance by medium-power states, constrains the security power gap with the superpowers, and solidifies the international security situation.

2.1 Security implications of military AI

(1) Increasing competition for military power

Technology is an important driver of military revolutions, and in successive military revolutions, the cumulative effects of technological advances and military innovations usually trigger military revolutions when new technologies are applied to military systems and combined with the actions of military innovations (Krepinevich, 1994). The proliferation of AI has impacted the distribution of military power, with States being able to utilize new technology iterations to rapidly upgrade their capabilities and gain dominance and military advantage as military powers. Gaining a “first-mover advantage” is one of the most frequently mentioned concepts when discussing the overall AI arms race among the world’s developed countries, and this is particularly relevant to the potential for military AI (Thornton & Miron, 2020).

Inventing and pioneering the use of technology does not guarantee an advantage in international politics, and the difference between introducing technology to the battlefield and fully integrating it into a national strategy often determines success or failure in global politics (Horowitz, 2010). Enhancing military security capabilities through AI has been reflected in the military strategies of states, they are striving to develop AI technologies to ensure that their military capabilities are on par with or exceed those of their potential adversaries, to form pre-emptive military defense capabilities and deterrence capabilities, and to prevent their adversaries from gaining significant power advantages.

The dual-use nature of AI also provides a tool for adaptation and flexibility in the competition for military power. Civilian AI technologies can be used in several military domains, such as autonomous drones, AI-powered cyber weapons, and smart targeting systems. Advances made in civilian AI applications have the potential to be adapted or repurposed for military purposes for states to gain dual advantages in both the civilian and military domains and to gain a dominant position in the military power competition (Besenyő & Málnássy, 2024).

(2)Changing the traditional view of military security

Narrative discourse choices for military AI may lead to the reproduction of security dilemmas in terms of national security policy preferences. Securitization theory suggests that an actor's choice of security discourse on material resources such as armaments determines whether a deterrence strategy is successful or not (Yue, 2021). Based on different levels of deterrence needs, there is a large ambiguity in a state's interpretation of its military power. Kissinger has argued that, unlike conventional military weapons, the clandestine and ephemeral nature of AI means that it is not something that state actors can simply put on the table as an obvious threat. The combination of AI and military behavior makes the discourse of national security narratives more secretive and complex, and national security risk assessments may evolve into “black box” reasoning, which, under the influence of security dilemmas, can lead to a more offensive strategy for the development of military AI and influence the formulation of national security policies.

To seek moral support, the selective narrative of technology and weapons among states is closely related to the discursive power in the creation of rules in emerging areas. In the absence of uniform institutional norms, to win the tug-of-war over discursive power, states with first-mover advantages may set discursive traps, exaggerate or ignore the risks of technology, and engage in the game of institutional dominant power and interpretive power. Under the conflict of interests, the suspicion of other states’ development of AI weapons, their respective claims on the boundaries of the autonomy of smart weapons, and their interpretations of their actions to promote the military application of AI all influence the policy tendency of the state, some states may accelerate the development and deployment of new types of smart weapons, triggering an arms race for smart weapons and bringing about new security dilemmas.

(3) Spawning “algorithmic warfare” and other warfare

Driven by AI technology, “algorithmic warfare” is emerging around the traditional battlefield. The technology base of AI is more advanced, and its response to scenarios is more rapid, making the acquisition of combat information more accurate and the efficiency of military operations significantly improved (Downey,2024). Autonomous weapon systems have been rapidly developed and applied in the actual battlefield, and the combination of intelligent systems for recognizing and analyzing battlefield data, drone operations, and robot soldiers with existing weapons has significantly improved the military’s combat power.

The algorithmic attack and defense competition in virtual space is becoming increasingly fierce. The field of artificial intelligence military applications beyond the traditional geographic space, extended to virtual cyberspace, through the machine scale and artificial intelligence technology to enhance the attack and defense capabilities, has become a new heights of the great powers competing in cyberspace.

Military AI has great potential for cognitive warfare if one or both sides use these technologies to interfere in the other's domestic political affairs. In the Russia-Ukraine crisis, the use of AI-generated social accounts to spread disinformation has greatly increased, further demonstrating the multiplier effect of AI in cognitive warfare.

2.2 Regulatory issues in the military application of artificial intelligence

(1) Risk of “arms autonomy” for non-state actors

Stewart Russell has warned that the biggest winners in the AI arms race will be “small rogue states and non-state actors such as terrorists” (Ross, 2018). When AI is combined with traditional concepts of state power, such as military and weapons, the power of actors is also increasingly intertwined with their expertise and investment in the field of AI, presenting the development of multiple actors overlapping and competing with each other in terms of global governance.

Large commercial corporations have a strong ability to allocate technology, data, talent, and other resources. These multinational corporations have the data ecosystems and cutting-edge talent that can enable technological breakthroughs, even if only for commercial gain, it will further benefit if these technologies can be diverted to military use. Multinationals have no allegiance to nation-states but rather move globally, settling

wherever there is a market advantage (Hurst & Hompson, 2002). To some extent, this allows them to determine which states gain an advantage in military AI.

Non-state actors have demonstrated a certain degree of autonomy in the development and governance of AI weapons. Due to the low threshold of access, terrorists may misuse smart weapons for attacks. This is centered on the resurgence of international violence by non-state actors in the form of terrorism and organized crime (Ilijevski et al., 2023). Terrorists have demonstrated the ability and intent to invent and utilize innovative technologies in combat, a development that will continue with the advancement of AI technology, which has already seen the emergence of drone swarming, and the use of smart weapons by terrorists is expanding the scope of the threat with the emergence and popularity of easily accessible (Besenyő, 2021).

Terrorists have also demonstrated a certain degree of sensitivity in the use of artificial intelligence to create "cyber-terrorism" on the Internet using smart technologies. As transnational criminal activities in cyberspace are more insidious, use mostly cryptocurrencies as settlement tools, involve more complex governance actors, and terrorist organizations have never ceased their attempts to circumvent the existing cyber firewalls, the fight against such activities especially needs to be countered with smarter technologies.

(2)Ethical issues

The rapid escalation of militarized AI applications is a serious risk. Algorithms are by no means safe, they are not immune to the risk of malware attacks, nor are they immune to the errors, biases, and manipulations that post-phenomenology suggests shape virtually all of humanity's relationship with the world by technologies that influence our decision-making horizons in existential ways (Ihde, 2009). When rules contradict each other, AI military systems can cause complex and unpredictable damage to unwanted people and critical infrastructure. As algorithms continue to be upgraded, the question of how to ensure that intelligent military systems adhere to humanitarian principles and maintain justice further expands the scope of the security problem.

The development of laws for military AI also faces new ethical tests. The emergence of military AI may further lead to a decoupling of conduct and responsibility in war, challenging the human rationality and humanism in international law established by the

Malton Clause and the Geneva Conventions has further integrated.[3] According to the Airwars, at least 22,679 civilians, and possibly as many as 48,308, have been killed by U.S. drones and airstrikes (Piper & Dyke, 2021). The use of AI in military operations does not circumvent the goal of innocence, and issues such as how to fill the gaps in existing laws and provide accountability and recourse for wrongdoing in the military application of AI are serious challenges for traditional legal ethics.

Overall, the military application of artificial intelligence has posed unprecedented new challenges to military security, political security, network security, information security, ethical security, and other fields in geographic space and virtual space, presenting a situation of blurred boundaries in which traditional and non-traditional security issues are mutually encompassing and intertwined. States have also shown different attitudes towards the use of AI to enhance military capabilities and the regulation of associated risks.

3. Beyond security: EU military AI security capacity-building

Against the backdrop of a deteriorating geopolitical environment, the EU's discussions on "strategic autonomy" and "technology sovereignty" are also broadly concerned with intelligent innovations in defense technologies, with greater emphasis on developing the potential of AI for military security capacity building.

3.1 Strengthening the EU Common Defense Capabilities

The deterioration of the geo-security environment and anxieties about military-technology innovation have prompted the EU to further promote the embedding of technologies such as artificial intelligence in the defense system. In recent years, the EU's orientation towards its self-identity in the field of defense and security has been shifting as the risk of war reappearing on European soil increases. Internal and external political upheavals, such as the unpredictable and insecure international security landscape and the rise of war crises, have further amplified Europe's pervasive state of ontological (insecurity) and a growing sense of existential fear and security anxiety (Kinnvall et al., 2018). The EU has positioned itself as "a stronger and more capable security provider" in response to major

[3] The main thrust of the provision is that, between armed conflicts, both civilians and combatants shall be protected and governed by the principles of international law as they derive from the requirements of governance, humane regulations and public conscience established between civilized nations.

geopolitical shifts and growing security challenges in Europe (Council of the European Union, 2022). The Russia-Ukraine crisis in 2022 has further impacted the EU's view of security, with modern warfare, territorial defense, and military deterrence being unavoidable realities in the EU's defense domain. On the military technology front, the strategy of utilizing cutting-edge civilian or dual-use technologies to bridge the military-technology innovation gap between Europe and other major powers is reflected in several EU decisions. The EU has actively pursued a market-driven strategy to revamp the relatively lagging European defense technology and industrial base and has encouraged research and innovation in technologies with significant military impact potential, such as AI, to create a pool of technologies shared between military and civilian uses (Csernatoni, 2018). Senior officials in the EU defense system also recognize that AI could be a real opportunity for the EU to strengthen its common security and defense capabilities, suggesting that AI can reduce costs, mitigate the risk of conflict, improve the EU's defense capabilities, and protect human rights in military operations (European Defence Agency, 2019). Emerging security technologies, such as AI, are being used as an important tool for defending Europe's security as well as preserving the EU's innovative edge and the creation of a state of security by focusing on AI technology innovations in security, defense, and military capacity building is both a reflection of the EU's strengthened security consensus and an important way for the EU to enhance its common security and defense capabilities.

The double overlaying trend of strategic autonomy claims in the field of defense and the building of technology sovereignty has made artificial intelligence a breakthrough for the EU in upgrading its military security capabilities. The concept of EU strategic autonomy is often associated with security and defense matters, "the EU must have the capacity to act autonomously, backed up by credible military forces, and the means to decide on the use of these forces in response to international crises." The EU seeks to propose a pragmatic and autonomous approach to avoid dependence and geopolitical coercion in key technology sectors, to progressively identify greater responsibility for its security, and to act strategically in the field of defense to increase its capacity for autonomous action (European Council, 2022). In this context, the prioritization of dual-use and emerging disruptive technologies has played a central role in the formation of the "technology regime"(Hecht, 1998). The shift towards the integration of high-political matters related to European security and defense with broader industrial, technology, and digital-related fields has contributed to the growing role of the European Commission as a supranational institutional

actor in defense and technology governance. Maintaining a leadership role in emerging technologies such as artificial intelligence is critical to the EU's overall security autonomy and technology strength and is a major legitimizing incentive for more policy initiatives at the EU level. The continued enhancement of the EU's technology autonomy in high-tech and its broader applicability in the security domain is an important consensus among EU Member States on defense transformation.

3.2 Improve the institutional system and increase financial support

Given the importance of technologies such as AI for the strategic autonomy and technology sovereignty of the EU's military domain, the EU's AI strategy and the strategic autonomy plan for defense also further emphasize the need to reduce dependencies in key technology areas and to improve supply chain security in all areas (European Commission, 2021a). The sense of urgency in responding to geopolitical and technological change further highlights the strategic importance of indigenous emerging and dual-use technologies, including interest in European security integration and high-end defense technology and industrial issues (European Commission, 2021b). To this end, the EU has progressively increased its investment in military AI research and development.

To strengthen the financial support for cooperation in the field of security and defense, since 2016, the EU has started a new chapter of defense integration and research and development of indigenous European security technologies (Karampekios et al., 2018). Federica Mogherini presented the global strategy for EU foreign and security policy in 2016, followed by the Security and Defense Implementation Plan (SDIP), which sets out a series of practical actions to advocate for the creation of a financial instrument to fund investment in cross-border research projects and the development of advanced European security technologies to foster a competitive and innovative industrial base (European Union Global Strategy, 2016). The Council of the European Union further emphasized the need to improve the structure of the EU's Common Security and Defense Policy (CSDP), including military planning and operational capabilities, as well as security and development capacity building. A Decision on Permanent Structured Cooperation (PESCO) was adopted, with the 25 participating member states agreeing on an initial list of 17 defense cooperation projects covering the areas of training, capacity development, and operational readiness in the field of defense (Council of the European Union, 2017a). As a follow-up, the Council also agreed on the proposed regulation to create the European Defense Industry Development

Program (EDIDP), aimed at supporting the competitiveness and innovation capacity of the EU defense industry as part of the European Defense Fund (EDF) (Council of the European Union, 2017b). The creation of the EDF further strengthens financial support for intra-EU cooperation in defense technology innovation, financially enhances the EU's autonomy in defense technology and industry, and boosts the EU's research and innovation capabilities in disruptive defense technologies. In EDF's 2021-2027 work plan, the budget for funding collaborative defense technology research has reached 2.7 billion Euros (EDF, 2024). In February 2021, the European Commission presented its Action Plan on Synergies in the Civil, Defense, and Space Sectors, which proposes a more transversal and cross-cutting approach to promote research and technology development to enhance the EU's overall innovation capacity (European Commission, 2021a). Starting in the first half of 2022, to support the development of disruptive technologies such as artificial intelligence, the European Commission proposed new forms of innovation funding to facilitate the involvement of non-traditional players, attract start-ups, and promote cross-fertilization of solutions, as well as to take advantage of the opportunities offered by EU programs and instruments, including the Digital Europe Program (DEP) and EDF (European Commission, 2021a). In July 2022, the European Commission announced that it would provide €1.2 billion in funding from EDF to projects related to the use of technologies such as AI for defense (European Commission,2022). EU member states are also collaborating on military AI projects, for example, the Future Combat Air System (FCAS), which is being developed by France, Germany, and Spain (Airbus, 2020). These collaborations between member states facilitate the integration of relevant resources within the EU, reduce the cost of knowledge and investment in military AI-related innovations, and enhance interoperability between EU armed forces.

On the other hand, EU AI documents emphasize “safety” rather than “security” and do not distinguish between the two concepts as they are used in different fields and different contexts (Andrasko et al., 2021). In the context of the further deconstruction of AI and its discourse, the blurred lines between civilian and military technologies also make it difficult to distinguish whether investments in AI forces are used for military security purposes. However, it is certain that EU investments in military AI are in the minority and have become more important because of the tense geopolitical situation.

4. Under regulation: regulatory norms for military AI in the EU

Regulation is an important tool in technology security policy, and the rise of the EU as a "Regulatory Security State" (RSS) reflects a mode of operation in EU politics where member states' hesitancy to transfer financial or military capabilities to the supranational level has led EU authorities to turn to regulation as a positive alternative tool in terms of shaping global political influence (Majone, 1994). The close relationship between technology, military equipment, and operational efficiency has driven the logic of securitization to gradually penetrate the field of technical regulation, where technology development has been increasingly securitized and constructed as a security-relevant object over the past decades (Wæver, 1995). As a general-purpose technology with dual-use applications, the power to regulate AI will affect geopolitical competition to some extent, and the EU has been building its AI regulation. And how to regulate the more secretive military AI is also a question that the EU is exploring.

4.1 Constructing a self-restraint image to develop rules for military AI governance

The EU outperforms other states and regions when it comes to legal, ethical, and responsible regulation of AI. As far as the regulation of AI is concerned, the EU aims to replicate the successful model of the GDPR and position itself as a global standard-setter (Hobbs, 2020). The European Commission has proposed the Artificial Intelligence Act, which regulates and restricts the application of AI according to risk levels. The EU's early layout and focus on AI governance increases its advantage in setting regulatory standards, and its early and future legislation could influence global AI regulatory standards.

The regulation of military AI has progressed more slowly relative to civilian AI, but the experience of regulating civilian AI can serve as a foundation for developing rules for military AI. In the EU, the issue of the arms control agenda involves the cession of defense powers by member states and falls under the CFSP and the CSDP, where member states are the key actors in achieving and maintaining common regulatory rules (Biedenkopf et al., 2021). This requirement for consistency in member-state decision-making also explains why the EU's AI strategy makes no mention of the regulation of military AI. The European Commission has made considerable efforts to develop rules for the governance of civilian AI, which provide a potential foundation for the EU's work on regulating the responsible military use of AI.

The EU is building an image of self-restraint concerning the EU's regulatory objectives for military AI, intending to make the EU a role model for the responsible development, adoption, and use of AI while ensuring the EU's competitiveness in this field. Through the EU's specific rules on the regulation of civil AI, the rules on the responsible military use of AI should also comply with the "legality" requirement of respecting all applicable laws and regulations, be consistent with the EU's principles and values, and preserve the "human-center" of human agency and oversight in the use of AI systems. "human-center" in the use of AI systems, and "stability" in terms of technical safety. EU officials have also specifically emphasized the importance of a ban on LAWS. In its guidance on the use of military AI, the EU Parliament emphasized the need to respect human dignity and human rights in all EU defense-related activities. Systems supporting AI must allow humans to exert meaningful control so that they can be held responsible and accountable for their use (European Parliament, 2021a). The use of lethal autonomous weapons systems raises fundamental ethical and legal questions about human control. They reiterate their call for The EU to develop a strategy to ban them and ban so-called "killer robots." The decision to select targets and use autonomous weapons systems for lethal action must always remain under human control.

The EU has expressed an expectation to take a leading role in creating and promoting a global framework governing military AI. For example, the European Parliament has adopted two resolutions that express "the ambition to maintain control over the regulations to be developed so that they are not forced to adopt or accept standards set by others" (European Parliament, 2021b). In its position to regulate military AI, the EU portrays itself as the rule maker for military AI, with rules that represent European values and can lead to international regulation.

4.2 Set multi-participant network to facilitate consensus-building

For AI governance, the EU's focus on multi-party participation in AI regulation, particularly the construction of networks of expertise, is an important way of constructing the EU's military AI regulatory path.

Leveraging expertise to inform regulation as government is an important process in the development of technology regulatory rules in the EU. In 2018, the EU formed two expert groups to provide expertise for governance rules on artificial intelligence: the High-Level Expert Group on AI (AI HLEG) and the Global Tech Panel (GTP). The AI HLEG and GTP

are composed of members from multiple stakeholder groups, including industry associations, academia, business, and civil society representatives, to take into account the interests of all parties so that technologists' opinions can be fully considered in regulatory rule-making. The AI HLEG has provided several recommendations for the EU's drafting of documents related to the governance of general-purpose AI. In 2019, the AI HLEG presented the "Ethics guidelines for trustworthy AI," which was an important source of input for the EU's white paper on AI, proposing to create a trustworthy and safe general AI regulatory framework. The AI HLEG specifically recommends that the development of military AI should be limited and regulated to meet standards (European Commission, 2019a). The EU describes the GTP as "bringing together leaders from the tech industry, the investment world, and civil society" (European Union External Action, 2018a). The GTP's mandate focuses on "the link between technology and the CFSP." Mogherini emphasized the group is dedicated to "regulating the military application of new technologies" (European Union External Action, 2018a). This demonstrates the GTP's special position and strong influence on issues related to military AI and security in the EU.

Outside of specialized knowledge networks, bureaucracies within the EU are also pushing for consensus among member states on military AI regulation. In 2018, the EU adopted a resolution calling for a ban on LAWS (European Parliament, 2018). The Greens/EFA group is actively pushing within the European Parliament to make the budget of the EDF conditional on not allocating funds to LAWS R&D projects (Brzozowski, 2019). The Finnish Presidency of the Council of the European Union in 2019 called on member states to pay more attention to ethical considerations when thinking seriously about the impact of AI on the EU's defense strategy. In June 2020, the European Parliament agreed to set up a special committee on AI in the digital age to capture issues related to military AI. In 2021, MEPs proposed "Guidelines for military and non-military use of Artificial Intelligence," which provides relatively systematic recommendations on the development of AI for military use, including AI can neither replace human decision-making nor human contact, the need for an EU strategy to ban LAWS, and a call for the EU to take a leading role, together with the UN and the international community, in creating and promoting a global framework to govern the military use of AI. As the European Parliament's resolution on AI emphasizes, "AI used for defense purposes should be responsible, fair, traceable, reliable and governable"(European Parliament, 2021c).

The actions of these internal institutions can also contribute to the EU's construction of regulatory power to develop regulations, formulate strategies, and introduce norms in the field of military AI, demonstrating the position of the EU institutions as a normative power that prefers institution, rule and value-based responses to security issues.

4.3 Promoting international participation and opposing the AI arms race

The EU has been actively involved in the debate on the control of cutting-edge and emerging technologies, in 2013, the EU made its first statement on LAWS at the United Nations Human Rights Council, arguing that the use of autonomous weapons should be discussed in ethical, legal, operational and technical terms (Denk & Kayser, 2017). The EU further expressed its support through the Convention on Certain Conventional Weapons (CCW) and promoted the establishment of the Group of Governmental Experts (GGE) (Denk & Kayser, 2017). Since 2017, the CCW has conducted an international debate on LAWS in the form of GGE; the EU has advocated calling for these efforts to ensure compliance with international humanitarian law and human rights law at different stages of the life cycle of AI weapons or compliance with the principles of international humanitarian law, proportionality in the use of force and precautions before intervention (European Parliament, 2020). Attempts at direct regulation of military AI have been made by EU institutions, with two resolutions adopted by the European Parliament, including the statement that "systems without any human control and supervision must be prohibited in all circumstances without exception" (European Parliament, 2021b). In the international framework, the EU does not explicitly show a preference for military AI competition, cooperation, international law, respect for the legal system, compliance with established rules, the role of human rights, and multilateralism intersect in different EU documents.

Some EU member states are also actively seeking a leading position in the regulation of LAWS. The EU has not yet expressed a substantial common position on military AI at the CCW (Barbé & Badell, 2020). The EU already has several preparatory groups that coordinate the views of member states' representatives in CCW discussions on LAWS, namely CONOP, CODUN, and the EUMCWG. Regular meetings of these groups have made efforts to define a common position of the EU member states on this issue. Over the past few years, France and Germany have played a leading role in the preparation of the CCW informal expert meeting framework, organizing the submission of a reflection paper on the definition and key features of LAWS. The EU has further emphasized the

requirements of applying and complying with international law, in particular international humanitarian law and human rights law (European Union External Action, 2018b). Important questions were raised on building a common understanding of LAWS, raising important points on accountability, and strengthening human oversight and control.

Multilateralism is an important part of the EU's approach to military AI regulation. According to the EUISS, "the EU is likely to emphasize the importance of promoting multilateral responses to the use of AI for military purposes" (Fiott & Lindstrom, 2018). CCW is an important platform for promoting the EU's regulatory approach as an international standard, and the EU aims to influence and "actively participate in the ongoing international debate and propose to international partners a moratorium on offensive laws" (European Commission, 2019b). It is also a sort of EU response to the AI arms race, and disciplining the development of military AI in other states by advocating for stronger regulation in international arms control regimes can be seen as part of the EU's security agenda.

5. **Conclusion**

From the "command of the sea" to "command of the air" to "command of the information," and now the rise of "command of the intelligence," technology has always been the core driving force for the evolution of power theory. For the future brought by AI, pessimists and optimists have their own opinions, but it is clear that the impact of military AI on the security of international society far exceeds expectations, and the governance of military AI should be more forward-aware and more effective.

The EU's efforts on AI for military security are in a delicate balance with its regulatory philosophy of preventing an arms race in military AI. The EU is accelerating the development of AI technologies by promoting policy initiatives, encouraging cross-collaboration, creating specialized expert groups, and providing financing platforms to achieve transformation in the field of European military security. Despite the gap between Europe and military powers such as the United States in the field of AI technology, how to regulate the integration of related technologies with the military has become an important area of global strategic competition. The EU and its member states have engaged in regulatory rule discussions in a number of ways and have worked to develop European standards for the responsible military use of AI. Its capabilities in military AI regulation

could be expanded by exploring ways to meet safety standards for military applications of AI at the technical level.

Nevertheless, the European Union faces a complex and multifaceted challenge in balancing security and regulation within the realm of military AI governance. As advancements in artificial intelligence continue to reshape defense capabilities, the EU must navigate the intricate landscape of ethical considerations, security imperatives, and regulatory frameworks. Striking a balance between ensuring robust security measures and adhering to stringent ethical standards requires a nuanced approach that involves collaboration among member states, engagement with international partners, and active participation of civil society.

Firstly, the conflict between security needs and ethical responsibilities is especially pronounced. The application of artificial intelligence in the military can significantly enhance defensive capabilities and operational efficiency. However, an over-reliance on AI technology raises ethical and legal concerns. The EU must enhance military capabilities while ensuring these technologies are not misused, thereby avoiding strong opposition and distrust from the international community.

Secondly, there is the issue of coordination and consistency among member states. EU member states have significant differences in military strategy, resource allocation, and technology development. Some states may prefer to quickly deploy advanced AI technologies to enhance their defense capabilities, while others may prioritize ethical concerns and compliance with international law. This internal inconsistency could weaken the EU's unified stance and influence in global AI governance.

Moreover, the pressure of global competition exacerbates the EU's governance difficulties. Globally, especially driven by the US and China, the development of military AI technology is advancing at a rapid pace. If the EU acts too slowly in technology innovation and application, it may find itself at a disadvantage in international competition, affecting its global strategic position and security.

Additionally, public and civil society scrutiny and opposition are critical factors to consider. As public awareness of AI technology increases, so does the attention to the ethical and security issues related to its military application. Balancing the advancement of

military AI while addressing and mitigating public concerns and opposition and ensuring transparent and responsible technology use, becomes a pivotal issue in EU governance.

In summary, the EU's conundrum in military AI governance primarily lies in finding a balance between rapidly advancing technology applications and stringent ethical regulations. The EU needs to strengthen coordination and cooperation among member states, formulate unified and forward-looking policies, and actively participate in the development and promotion of international rules to resolve these dilemmas. By doing so the EU can maintain technology leadership while upholding its moral and legal standards in global governance, achieving the dual objectives of security and ethics.

References

1. Krepinevich, A. (1994). Cavalry to Computer: The Pattern of Military Revolutions. T he National Interest, (37). 30.
2. Thornton, R. & Miron, M. (2020). Towards the "Third Revolution in Military Affairs ": The Russian Military's Use of AI-Enabled Cyber Warfare. The RUSI Journal,165(3).18.
3. Horowitz, M. (2010). The Diffusion of Military Power: Causes and Consequences for International Politics. Princeton: Princeton University Press. 3.
4. Besenyő, J. & Málnássy, A. (2024). Geopolitical Dimension of Libyan Drone Warfar e: The Use of Turkish Drones on the North African Battlefields, Obrana a strategie, 24 (1). 3-1 7.
5. Yue, SS. (2021). Revisiting Securitization: Theoretical Dilemmas and New Explorati ons in Foreign Policy Discourse Analysis. Journal of International Relations, (3). 8.
6. Downey, A. (2024). Algorithmic predictions and pre-emptive violence: artificial intell igence and the future of unmanned aerial systems. Digital War, (5), 123-133.
7. Ross, D. (2018). Terrorists Are Going to Use Artificial Intelligence.Defense one. Def ense One, Available at: https://www.defenseone.com /ideas/2018/05/terrorists-are-going-to-us e-artificial-intelligence/147944/.
8. Hurst, P. & Hompson, G. (2002). Questioning Globalization: Possibilities for Internati onal Economics and Governance. Beijing: Social Science Literature Publishing House. 1.
9. Ilijevski, I. et al. (2023). The Weaponisation of Drones – A Threat from Above Used f or Terrorist Purposes. Journal of Criminal Justice and Security, (3). 336-349.
10. Besenyő, J. & Márton, K. (2021). Hospital Attacks Since 9/11: An Analysis of Terr orism Targeting Healthcare Facilities and Workers. Studies in Conflict & Terrorism, 47(1). 36 –59.
11. Ihde, D. (2009). Postphenomenology and technoscience: The Peking University Lec tures. New York:State University of New York Press. 23.
12. Piper, I. & Dyke, J. (2021). Tens of thousands of civilians likely killed by US in "Fo rever Wars". Airwars. Available at: https://airwars.org/news-and-investigations/tens-of-thousa nds-of-civilians-likely-killed-by- us-in-forever-wars/.

13. Kinnvall, C. et al. (2018). Introduction to 2018 Special Issue of European Security: Ontological (In)Security in the European Union. European Security, 27(3). 249-265.

14. Council of the European Union. (2022). A Strategic Compass for Security and Defen ce - For a European Union that protects its citizens, values and interests and contributes to inte rnational peace and security. Available at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.

15. Csernatoni, R. (2018). Constructing the EU's High-Tech Borders: FRONTEX and D ual-Use Drones for Border Management. European Security, 27(2). 180.

16. European Defence Agency. (2019). Presentation by Jean-François Ripoche at SEDE public hearing on Artificial Intelligence-enabled systems in security and defense. Available at: https://www. europarl.europa.eu/cmsdata/194142/SEDE_hearing_presentation_Ripoche_3Dec ember2019-original.pdf.

17. Franco–British St. Malo Declaration. Available at: https://www.cvce.eu/en/obj/franc o_british_st_malo_declaration_4_ december_1998-en-f3cd16fb-fc37-4d52-936f-c8e9bc80f24f .html

18. European Council. (2022). Informal meeting of the Heads of State or Government V ersailles Declaration. Available at:https://www.consilium .europa.eu/media/54773/20220311-v ersailles-declaration-en.pdf

19. Hecht, G. (1998). The radiance of France. nuclear power and national identify after World War 2. Cambridge:MIT Press.12.

20. European Commission. (2021a). Action plan on synergies between Civil, Defence, a nd Space Industries. Available at: https://ec.europa.eu/info/files/action-plan-synergies-betwee n-civil-defence-and-space-industries_en.

21. European Commission. (2021b) "2021 State of the Union Address by President von der Leyen. Available at: https://ec.europa. eu/commission/presscorner/detail/en/SPEECH_21_ 4701

22. N. Karampekios, et al. (eds.). (2018). The Emergence of EU Defence Research Polic y. from Innovation to Militarization. Cham:Springer International Publishing.

23. European Union Global Strategy. (2016). A Global Strategy for the European Union' s Foreign and Security Policy: Shared Vision, Common Action: A Stronger Europe. Available at: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

24. Council of the European Union (2017a), "Council Decision Establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States. A vailable at:http://www.consilium.europa.eu/media/32000/st14866en17.pdf.

25. Council of the European Union (2017b). European Defence: Council Agrees Its Posi tion on the Proposed Regulation Establishing the European Defence Industrial Development Pr ogramme (EDIDP). Development Programme (EDIDP). Available at:http://www.consilium.eu ropa.eu/en/press/press-releases/2017/12/12/european -defence-council-agrees-its-position-on-t he-proposed-regulation-establishing-the-european-defence-industrial-development-programme -edidp/pdf

26. EDF. (2024). Discover the EDF. Available at: https://defence-industry-space.ec.euro pa.eu/eu-defence-industry/european-defence-fund-edf_en

27. European Commission. (2021a). Action plan on synergies between Civil, Defence, a nd Space Industries. Available at: https://ec.europa.eu/info/files/action-plan-synergies-between -civil-defence-and-space-industries_en.

28. Ibid.

29. European Commission. (2022). Defence industry: EU takes steps to invest almost €1 .2 bn. Available at:https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4595.

30. Airbus. (2020). Future combat air systems: owning the sky with the next generation weapons system. Available at: https://www.airbus.com/en/newsroom/stories/2020-06-future-combat-air-system-owning-the-sky-with-the-next-generation-weapons

31. Andrasko, J. et al. (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: Challenges and opportunities for the EU Legal Framework. AI and Society, (36). 623-636.

32. Majone, G. (1994). The rise of the regulatory state in Europe. West European Politics, 17(3). 77-101.

33. Wæver, O. (1995). Securitization and desecuritization. In R. Lipschutz (eds.). On security. Columbia: Columbia University Press. 46-86.

34. Hobbs, C. (2020). Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry. ECFR. Available at:https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/

35. Biedenkopf, K. et al. (2021). Introduction: shades of contestation and politicization of CFSP. European security, 30(3). 332.

36. European Parliament. (2021a). Guidelines for military and non-military use of Artificial Intelligence. Available at: https://www.europarl.europa.eu/news/en/press-room/20210114IPR95627/guidelines-for-military-and-non-military-use-of-artificial-intelligence

37. European Parliament. (2021b). European Parliament resolution of 20 January 2021 on artificial intelligence. Available at: https://www.europarl.europa.eu/ doceo/document/TA-9-2021-0009_EN.html.

38. European Commission. (2019a). Ethics Guidelines for Trustworthy AI. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

39. European Union External Action. (2018a). Global tech panel: Mogherini starts debate with tech leaders. Available at: https://www.eeas.europa.eu/node/45483_en

40. European Parliament. (2018). European Parliament resolution of 12 September 2018 on autonomous weapon systems (2018/2752(RSP)). Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html#:~:text=European%20Parliament%20resolution%% of 20of%2012%20September%202018%20on,1%20of%201977%20additional%20to%20the%20Geneva%20Conventions%2C

41. Brzozowski A. (2019). European Defense Fund agreed amid ethics concerns. Available at: https://www.euractiv.com/section/defence-and-security/news/european-defence-fund-agreed-amid-ethics-concerns/

42. European Parliament. (2021c). "Report on artificial intelligence: Questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice, 2021/C 456/04. Available at: https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_EN.html.

43. Denk, S. & Kayser, D. (2017). Keeping control of European positions on lethal autonomous weapon systems. Available at: https://www.paxforpeace.nl/ publications/all-publications/keeping-control.

44. European Parliament (2020),"Framework of ethical aspects of artificial intelligence, robotics and related technologies, P9_TA(2020)0275. October 20, 2020, Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html.

45. European Parliament. (2021b). European Parliament resolution of 20 January 2021 on artificial intelligence. Available at: https://www.europarl.europa.eu/ doceo/document/TA-9-2021-0009_EN.html.

46. Barbé, E. & Badell, D.(2020). The European Union and lethal autonomous weapons systems: United in diversity? In EJ.Nogués et al. (eds.). European Union Contested. Norm Research in International Relations. Cham: Springer International Publishing. 133-152.

47. European Union External Action. (2018b). Group of governmental experts conventio n on certain conventional weapons: EU statement: Lethal Autonomous Weapons Systems (LA WS). Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/43045/group-g overnmental-experts-convention- certain-conventional-weapons-eu-statement-lethal_en

48. Fiott, D. & Lindstrom, G. (2018). Artificial Intelligence, what implications for EU se curity and defense? European Union Institute for Security Studies Brief. Available at:https://w ww.iss.europa.eu/content/artificial-intelligence-–-what-implications-eu-security-and-defence.

49. European Commission. (2019b). Policy and investment recommendations for trustw orthy AI. Available at:https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-re commendations-trustworthy-artificial-intelligence

50. Johnson, J. (2019). Artificial intelligence & future warfare: implications for internati onal security. Defense & Security Analysis, 35(2).147-169

51. Geist, E.&Lohn, A. (2018). How Might Artificial Intelligence Affect the Risk of Nu clear War?. Santa Monica CA: RAND Corporation

52. Horowitz, M. (2018). Artificial Intelligence, International Competition, and the Bala nce of Power. Texas National Security Review, 1(3). 37-57

53. Cave, S.&ÓhÉigeartaigh, S. (2017). An AI Race for Strategic Advantage: Rhetoric a nd Risks. Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society

54. Roff, H. (2014). The Strategic Robot Problem: Lethal Autonomous Weapons in War . Journal of Military Ethics, 13(3). 211-227

55. Horowitz, M. (2019). When speed kills: Lethal autonomous weapon systems, deterre nce and stability. Journal of Strategic Studies, 42(6). 764-788

56. Scharre, P.(2023) Four Battlegrounds: Power in the Age of Artificial Intelligence. N ew York:W. W. Norton & Company

57. Anderson K.&Waxman, M. (2017). Debating Autonomous Weapon Systems,Their E thics,and Their Regulation Under International Law. In R. Brownsword & E. Scotford & K.Ye ung (eds.). The Oxford Handbook of Law, Regulation,and Technology. Oxford:Oxford Univer sity Press; Scharre, P. How swarming will change warfare. Bulletin of the Atomic Scientists,7 4(6). 385-389

58. Stix, C. & Maas,M. (n.d.) Bridging the gap: the case for an "Incompletely Theorized Agreement" on AI policy. AI and Ethics, (1). 261-271

59. Schmitt, L. (n.d.) Correction to: Mapping global AI governance: a nascent regime in a fragmented landscape. AI and Ethics, (2). 303–314

60. Schiff, D.et al. (2020). What's Next for AI Ethics, Policy, and Governance? A Globa l Overview. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society

61. Stefan, L. (2020). On the Governance of Artificial Intelligence through Ethics Guide lines. Asian Journal of Law and Society, 7(3). 437-451