SCHOOL OF ECONOMICS, BUSINESS AND INTERNATIONAL STUDIES

DEPARTMENT OF INTERNATIONAL AND EUROPEAN STUDIES

POSTGRADUATE PROGRAM IN INTERNATIONAL AND EUROPEAN STUDIES

MASTER THESIS

Artificial Intelligence (AI) Application in the Security Field: Legal and Ethical Implications for the European Union

Eleni Makri

ΜΘ22018

Supervising Professor: Associate Professor Mr. Liaropoulos Andreas

Three-Member Committee:

1. Professor Emeritus Mr. Liakouras Petros
2. Associate Professor Mr. Liaropoulos Andreas
3. Assistant Professor Mr. Konstantopoulos Ioannis

Piraeus, 2025

Υπεύθυνη Δήλωση / Solemn Declaration:

Βεβαιώνω ότι το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία είναι, αποκλειστικά, ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται, έχουν αντληθεί από άλλες πηγές και έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον τελώ εν γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου αφαιρείται ανά πάσα στιγμή, αμέσως, ο τίτλος.

Η δηλούσα,

Ελένη Μακρή

The intellectual work fulfilled and submitted based on the delivered master thesis is exclusive property of mine personally. Appropriate credit has been given in this diploma thesis regarding any information and material included in it that have been derived from other sources. I am also fully aware that any misrepresentation in connection with this declaration may at any time result in an immediate revocation of the degree title.

Signed,

Eleni Makri

To my parents

TABLE OF CONTENTS

Abstract

This thesis examines the application of Artificial Intelligence (AI) in the security field, with a particular focus on the European Union as a regulatory and strategic actor within the broader international security environment. It argues that AI constitutes not merely a technological innovation but a structural force reshaping military operations, internal security practices, and the governance of risk across Europe. Drawing on realism, liberalism, and constructivism, the study situates AI at the intersection of geopolitical competition, institutional governance, and normative contestation, highlighting the distinctive role of the EU in promoting human-centric and rights-based approaches to AI governance.

The analysis explores key AI-enabled security applications in military affairs, cybersecurity, and hybrid threats, with particular attention to autonomous systems, data-driven surveillance, and algorithmic decision-support tools. A case study of the Russia–Ukraine war is employed to illustrate the operational relevance of AI-enabled capabilities, including drones, intelligence systems, cyber operations, and influence activities, while also exposing vulnerabilities, escalation risks, and strategic dependencies relevant to European security.

The thesis further examines the legal implications of AI through the lenses of international humanitarian law, human rights law, and European Union law. Particular emphasis is placed on the EU Artificial Intelligence Act and its interaction with existing regulatory frameworks such as the General Data Protection Regulation, highlighting challenges related to accountability, proportionality, and civil–military governance asymmetries. Ethical considerations, including the responsibility gap, meaningful human control, and the diffusion of digitally authoritarian practices, are assessed in light of the EU's normative commitments. The thesis concludes that the effectiveness of the EU's approach depends on its ability to align regulatory leadership with security capabilities, strengthen institutional oversight, and sustain credible international norms while preserving democratic values.

Keywords

Artificial Intelligence; European Union security; EU Artificial Intelligence Act; autonomous weapons systems; strategic autonomy

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει την εφαρμογή της Τεχνητής Νοημοσύνης (ΤΝ) στον τομέα της ασφάλειας, με ιδιαίτερη έμφαση στην Ευρωπαϊκή Ένωση ως ρυθμιστικό και στρατηγικό δρώντα στο ευρύτερο διεθνές περιβάλλον ασφάλειας. Υποστηρίζεται ότι η ΤΝ δεν αποτελεί απλώς τεχνολογική καινοτομία, αλλά διαρθρωτικό παράγοντα που αναδιαμορφώνει τις στρατιωτικές επιχειρήσεις, τις πρακτικές εσωτερικής ασφάλειας και τη διακυβέρνηση του κινδύνου στην Ευρώπη. Βασιζόμενη στις θεωρητικές προσεγγίσεις του ρεαλισμού, του φιλελευθερισμού και του κονστρουκτιβισμού, η μελέτη τοποθετεί την ΤΝ στο επίκεντρο της γεωπολιτικής ανταγωνιστικότητας, της θεσμικής διακυβέρνησης και της κανονιστικής αντιπαράθεσης, αναδεικνύοντας τον ρόλο της Ευρωπαϊκής Ένωσης στην προώθηση ανθρωποκεντρικών προσεγγίσεων που βασίζονται στα θεμελιώδη δικαιώματα.

Η ανάλυση εστιάζει σε βασικές εφαρμογές της ΤΝ στον τομέα της ασφάλειας, όπως οι στρατιωτικές χρήσεις, η κυβερνοασφάλεια και οι υβριδικές απειλές, με έμφαση σε αυτόνομα συστήματα, συστήματα επιτήρησης βασισμένα σε δεδομένα και αλγοριθμικά εργαλεία υποστήριξης λήψης αποφάσεων. Η μελέτη περίπτωσης του πολέμου Ρωσίας–Ουκρανίας αξιοποιείται για να καταδειχθεί η επιχειρησιακή σημασία των δυνατοτήτων που υποστηρίζονται από την ΤΝ, καθώς και οι σχετικοί κίνδυνοι κλιμάκωσης και στρατηγικής εξάρτησης για την ευρωπαϊκή ασφάλεια.

Η εργασία εξετάζει επίσης τις νομικές και ηθικές επιπτώσεις της ΤΝ μέσω του διεθνούς ανθρωπιστικού δικαίου, του δικαίου των ανθρωπίνων δικαιωμάτων και του δικαίου της Ευρωπαϊκής Ένωσης, με ιδιαίτερη αναφορά στον Κανονισμό της ΕΕ για την Τεχνητή Νοημοσύνη. Τέλος, καταλήγει στο συμπέρασμα ότι η αποτελεσματικότητα της ευρωπαϊκής προσέγγισης εξαρτάται από την ευθυγράμμιση της ρυθμιστικής ηγεσίας με τις επιχειρησιακές δυνατότητες ασφάλειας, τη θεσμική εποπτεία και τη διατήρηση των δημοκρατικών αξιών.

Λέξεις-Κλειδιά

Τεχνητή Νοημοσύνη; Ευρωπαϊκή Ένωση και ασφάλεια; Κανονισμός ΤΝ της ΕΕ; αυτόνομα οπλικά συστήματα; στρατηγική αυτονομία

1. INTRODUCTION

1.1 Background and Relevance

Artificial intelligence has emerged as one of the most transformative forces in contemporary international politics and security. Advances in data processing, algorithmic learning, and computational power have positioned AI as a central driver of military innovation, economic competitiveness, social governance, and geopolitical influence. As Allen and Chan (2017) and Pauwels (2020) demonstrate, global competition for AI advantage has become a defining feature of the twenty-first-century security environment, shaping strategic doctrines and power hierarchies at both regional and international levels. Increasingly, the capacity to exploit data, algorithms, and autonomous systems influences how states deter, defend, and project power.

From a security perspective, AI signals a structural shift comparable to previous military revolutions, such as the advent of nuclear weapons and the emergence of cyber warfare. AI-enabled systems can compress decision-making cycles, automate threat detection, expand surveillance capacity, and introduce varying degrees of autonomy into weapons platforms (Boulanin, 2019; Scharre, 2018; Johnson, 2019). These developments challenge conventional assumptions about human-centered warfare and generate unprecedented legal and ethical dilemmas regarding accountability, proportionality, and responsibility. As Schmitt and Thurnher (2013) and Arkin (2010) argue, the increasing autonomy of weapon systems places pressure on the law of armed conflict, which remains fundamentally anchored in human judgment and intent.

The geopolitical dimension of AI is particularly visible in the strategic competition among major powers. China, the United States, and Russia treat AI as a core national security asset, integrating it into military modernization programs, surveillance infrastructures, and information warfare strategies (Kania, 2017; Bendett, 2023). In parallel, authoritarian regimes increasingly deploy AI to consolidate domestic control and extend influence externally, reinforcing what Liaropoulos (2022) describes as “digital authoritarianism”. In this environment, AI functions not merely as a technological development but as a geopolitical variable shaping strategic priorities and political leverage.

Within this evolving global landscape, the European Union occupies a distinctive position. Unlike major military powers, the EU has sought to assert influence primarily through regulation and norm-setting rather than technological dominance. This strategy reflects the concept of Normative Power Europe articulated by Manners (2002), according to which the EU seeks to shape international behavior through values, rules, and legal standards. The regulatory leadership of the EU in digital governance is further captured by Bradford’s (2020) concept of the “Brussels Effect,” whereby European regulatory standards become de facto global benchmarks due to the size and attractiveness of the EU market. The adoption of the General Data Protection

Regulation in 2016 and the Artificial Intelligence Act in 2024 exemplify this projection of regulatory power (European Union, 2016; European Union, 2024).

At the same time, the EU increasingly recognizes that regulatory influence alone is insufficient in a security environment marked by technological rivalry, hybrid threats, and the integration of AI into military capability. The pursuit of digital sovereignty and strategic autonomy has therefore moved to the centre of European policy discourse (Fiott, 2018; Csernatoni, 2021; Liaropoulos, 2021). Digital sovereignty refers to Europe's capacity to control critical digital infrastructures, data ecosystems, and technological dependencies, while strategic autonomy extends this control into defence, security, and crisis management capabilities.

This dual identity of the EU as both a normative regulator and an emerging strategic actor generates inherent tensions. On the one hand, the Union promotes human-centric, rights-based AI governance through the Ethics Guidelines for Trustworthy AI (European Commission, 2019), the UNESCO Recommendation on the Ethics of AI (UNESCO, 2021), and the risk-based regulatory model of the AI Act. On the other hand, the EU faces mounting pressure to accelerate military innovation in AI in response to the operational lessons of the Russia–Ukraine war and the rapid militarization of autonomy (Csernatoni, 2024; Liaropoulos, 2024).

The relevance of this thesis lies precisely at this intersection between technological acceleration, security transformation, legal adaptation, and ethical contestation. AI in the security field does not merely raise technical questions of efficiency or performance; it reshapes the political economy of security, the conduct of warfare, the nature of threats, and the foundations of legal and moral responsibility. As Matthias (2004) and Sparrow (2007) argue, autonomous systems introduce a profound "responsibility gap," whereby harmful outcomes may no longer be easily attributable to identifiable human agents. This concern becomes particularly acute when lethal force is involved.

Moreover, AI expands the scope of security beyond the battlefield. Predictive policing, biometric surveillance, social media manipulation, and algorithmic profiling increasingly connect internal security with hybrid warfare and influence operations (Europol, 2023; Feldstein, 2019; Kapsokoli, 2023). This convergence between military, cyber, and societal security underscores the necessity of an integrated analytical approach that transcends traditional disciplinary boundaries and integrates legal and ethical dimensions.

Against this backdrop, this thesis examines the application of artificial intelligence in the security field through the combined lenses of international security studies, European integration, international law, and ethics. It analyses how AI transforms the conduct of security operations, how existing legal frameworks respond to autonomous and data-driven systems, and how ethical governance can be preserved in an era of algorithmic power.

1.2 Methodology and Scope

This thesis adopts a qualitative, interdisciplinary methodological approach integrating international relations theory, legal analysis, security studies, and political ethics. The complexity of AI as a dual-use technology operating across military, cyber, and internal security domains necessitates such an integrated framework. No single discipline can adequately capture the strategic, legal, and normative implications of AI in contemporary security environments.

The primary method employed is qualitative document analysis. This includes systematic examination of key European Union legal instruments such as the General Data Protection Regulation (European Union, 2016), the Artificial Intelligence Act (European Union, 2024), and the Cybersecurity Act (European Union, 2019), alongside strategic policy documents including the EU Strategic Compass for Security and Defence (EEAS, 2022). Together, these sources provide insight into how the EU conceptualizes risk, autonomy, human oversight, and accountability in relation to AI-enabled systems.

The regulatory analysis is complemented by institutional opinions and reports from EU bodies and agencies, including the European Data Protection Supervisor, the Fundamental Rights Agency, ENISA, Europol, and the European Defence Agency. These materials provide insight into how AI is operationalized in cybersecurity, policing, surveillance, and defence innovation. In parallel, defence-related publications from institutions such as SIPRI, CNAS, CSIS, and the Carnegie Endowment provide contextual insight into the strategic implications of military AI, including deterrence dynamics, escalation risks, and strategic stability.

Secondary academic literature supports the theoretical framework and the broader conceptual analysis. Realist, liberal, and constructivist approaches to technology and security are drawn from classical and contemporary scholarship, including Manners (2002), Pauwels (2020), Smuha (2021), Boulanin (2019), Johnson (2019), and Liaropoulos (2021–2024). Ethical and legal debates are informed by works on autonomous weapons and responsibility, including Arkin (2010), Roff and Moyes (2016), Schmitt and Thurnher (2013), Sparrow (2007), and Matthias (2004).

A case study methodology is employed through the analysis of the Russia–Ukraine war. This conflict provides empirical grounding for the operational use of AI-enabled drones, autonomous or semi-autonomous targeting systems, cyber operations, and influence campaigns. The case study is used not as an exhaustive military analysis but as an illustrative example of how AI transforms real-world conflict and exposes regulatory and ethical vulnerabilities (Bendett, 2023; Bondar, 2025; ENISA, 2025; Csernatoni, 2024).

The scope of the thesis is primarily European, focusing on the EU's regulatory, strategic, and normative responses to AI in security. At the same time, the analysis

remains embedded within the broader global context of technological competition, recognizing that AI governance is inherently transnational. The thesis does not include classified materials, technical algorithmic analysis, or quantitative modelling, which constitute its principal limitations. Nevertheless, by triangulating policy documents, academic literature, and empirical case material, it provides a robust analytical foundation for assessing the legal and ethical implications of AI in contemporary security.

1.3 Structure

This thesis is structured into seven chapters that progressively develop a comprehensive analysis of AI in the security field.

Chapter 1 introduces the research problem, situates artificial intelligence within contemporary international and European security dynamics, and outlines the methodological framework. It establishes the geopolitical, legal, and ethical relevance of the topic and frames the EU as a key regulatory and strategic actor.

Chapter 2 develops the theoretical framework and reviews academic literature. It examines realism, liberalism, and constructivism as interpretative lenses for understanding AI's impact on security. It further explores the concepts of digital sovereignty, strategic autonomy, and human-centric AI, drawing on the scholarship of Manners, Bradford, Smuha, Liaropoulos, Kapsokoli, and others to situate the EU's regulatory model within global geopolitical competition.

Chapter 3 analyzes concrete applications of AI in the military, cybersecurity, and hybrid warfare domains. It examines autonomous weapons, battlefield digitization, intelligence-led policing, cyber operations, and influence campaigns, with a detailed case study of the Russia–Ukraine war illustrating the operational consequences of AI-enabled conflict.

Chapter 4 focuses on the legal implications of AI in security, addressing international humanitarian law, human rights law, and EU regulatory frameworks. It evaluates how autonomous systems challenge principles of distinction, proportionality, accountability, privacy, and due process.

Chapter 5 examines the ethical implications of AI in security, including the responsibility gap, meaningful human control, and the risks of digital authoritarianism and ethical externalization.

Chapter 6 analyzes the European Union's strategic and policy response, including strategic autonomy, defense initiatives, the Strategic Compass, and civil–military coordination challenges.

Chapter 7 concludes with a synthesis of findings and presents legal, ethical, and strategic policy recommendations, while also identifying directions for future research.

2. THEORETICAL FRAMEWORK AND LITERATURE REVIEW

2.1 Theoretical Approaches to International–European Security

Understanding the implications of artificial intelligence for contemporary security requires grounding the analysis within established theoretical traditions of International Relations. Realism, liberalism, and constructivism offer distinct yet complementary interpretations of technological change and its criticality for military power, international cooperation, and normative governance. Together, these perspectives provide an essential analytical framework for situating the European Union's evolving approach to AI within broader debates on strategic autonomy, digital sovereignty, and ethical regulation.

From a realist perspective, artificial intelligence is understood primarily as a strategic instrument with the potential to reshape power balances and intensify security competition among states. Military superiority increasingly depends on algorithmic advantage, access to large-scale data, and the integration of autonomy into weapons systems and command-and-control architectures (Allen & Chan, 2017; Boulanin & Verbruggen, 2017; Scharre, 2018). AI compresses decision-making cycles, enhances targeting precision, and enables forms of warfare that unfold at speeds exceeding human cognitive limits. This acceleration introduces new escalation risks and challenges traditional deterrence logics, as misperceptions or automated responses may trigger unintended conflict dynamics (Horowitz & Scharre, 2021).

Realist analyses further emphasize the arms-race dynamics associated with military AI development. Competition among major powers—most notably the United States, China, and Russia—reflects classical patterns of technological rivalry, where early advantages are perceived as decisive and incentives favor rapid deployment despite uncertainty (Kania, 2017; Bendett, 2023). Boulanin (2019) and Boulanin et al. (2020) warn that AI-enabled military systems, particularly autonomous weapons and advanced surveillance technologies, may destabilize strategic stability by lowering thresholds for the use of force and obscuring attribution.

Within the European context, realist pressures manifest in growing concerns about technological dependence and strategic vulnerability. Empirical analyses of EU defence policy reflect this dynamic, as Liaropoulos (2024) argues that military AI has become a decisive enabler of European strategic autonomy, as reliance on non-European defence technologies undermines both operational effectiveness and political sovereignty. Similarly, Csernatoni (2021) observes that the EU's increasing focus on defence technological sovereignty reflects a gradual shift from purely normative ambitions toward material capability development in response to an increasingly competitive geopolitical environment.

Liberal theory, by contrast, emphasizes the role of institutions, international law, and cooperation in managing the risks associated with emerging technologies. From this perspective, AI does not inevitably lead to instability but can be governed through regulatory frameworks, transparency mechanisms, and confidence-building measures. The European Union's regulatory approach exemplifies this logic through instruments such as the General Data Protection Regulation, the Cybersecurity Act, and the Artificial Intelligence Act, which seek to harmonize innovation with fundamental rights and societal protections (European Union, 2016; 2019; 2024). Smuha (2021) characterizes this process as a global "race to AI regulation," in which regulatory capacity itself becomes a source of strategic influence alongside technological development.

At the international level, liberal institutionalist logic is reflected in ongoing multilateral discussions on autonomous weapons systems. Within the framework of the United Nations Convention on Certain Conventional Weapons, states have sought to develop shared principles and norms to mitigate the risks posed by lethal autonomous weapons, even in the absence of binding legal prohibitions (United Nations Convention on Certain Conventional Weapons, 2017–2025). Although progress has been limited, these processes illustrate attempts to manage AI-related security dilemmas through dialogue, norm formation, and incremental governance rather than unilateral competition.

Liberal institutionalism also provides analyses of EU cybersecurity governance. Kapsokoli (2020) highlights how coordination among member states, EU agencies, and institutions is driven by a liberal logic of collective resilience, even as national sovereignty concerns continue to constrain deeper integration. In this sense, AI governance becomes both a regulatory and political project aimed at reconciling national interests with shared security objectives.

Constructivism adds a crucial normative dimension by focusing on the role of values, identity, and discourse in shaping security practices. From this perspective, AI systems are not neutral technological tools, but socially constructed artifacts embedded within political cultures and ethical frameworks. The EU's emphasis on human-centric AI reflects its self-conception as a normative power committed to fundamental rights, transparency, and accountability (Manners, 2002). This identity is institutionalized through initiatives such as the Ethics Guidelines for Trustworthy AI and reinforced at the global level through instruments like UNESCO's Recommendation on the Ethics of Artificial Intelligence (European Commission, 2019; UNESCO, 2021).

The global diffusion of EU norms can be understood through Bradford's (2020) concept of the Brussels Effect, whereby regulatory standards adopted within the EU acquire extraterritorial influence due to market size and regulatory credibility. At the same time, constructivist analysis helps explain the emergence of competing normative models of AI governance. Liaropoulos (2022) and Feldstein (2019) demonstrate how authoritarian and hybrid regimes promote alternative approaches to AI regulation that prioritize

control, surveillance, and political stability over individual rights, challenging liberal democratic norms at the international level.

Constructivism also sheds light on the role of transnational advocacy networks in shaping debates on military AI. Movements such as the Campaign to Stop Killer Robots have reframed autonomous weapons as an ethical and humanitarian issue, influencing public discourse and institutional positions within the EU and the United Nations (Campaign to Stop Killer Robots, 2018–2025; Arkin & Sharkey, various years). These advocacy efforts illustrate how norms surrounding accountability, human dignity, and meaningful human control are socially constructed and politically contested.

Contributions from European and Greek scholars further reinforce this theoretical synthesis. Kapsokoli's work underscores the EU's ongoing struggle to reconcile sovereignty and integration in cybersecurity and digital governance, while Liaropoulos emphasizes how AI's military applications are reshaping debates on European strategic autonomy and defence cooperation (Kapsokoli, 2020; Liaropoulos, 2024). Together, these perspectives illustrate how theoretical approaches translate into concrete policy dilemmas within the European security architecture.

Taken together, realism, liberalism, and constructivism demonstrate that artificial intelligence is simultaneously a strategic instrument, a regulatory challenge, and a normative battleground. Understanding these theoretical perspectives is essential for analyzing the EU's legal, ethical, and strategic responses to AI and for situating European security policy within the broader evolution of international order.

2.2 AI and the Evolution of Security Studies

The emergence of artificial intelligence has contributed to a profound transformation of security studies, expanding the field beyond its traditional focus on kinetic military force and territorial defence. AI reshapes how threats are identified, interpreted, and addressed, blurring distinctions between military and civilian domains, internal and external security, and war and peace. As Johnson (2019) argues, AI-driven systems challenge foundational assumptions about speed, control, and human agency in conflict, requiring security studies to adapt both conceptually and analytically.

At the military level, AI accelerates the evolution of warfare by enabling advanced intelligence, surveillance, and reconnaissance capabilities, predictive logistics, autonomous navigation, and algorithmic targeting. Boulanin (2019) and Boulanin et al. (2020) highlight that AI progressively redistributes functions along the kill chain, shifting tasks traditionally performed by humans toward automated systems. This transformation compresses decision-making cycles and increases operational tempo, reinforcing concerns about escalation dynamics and crisis instability. Scharre (2018) similarly emphasizes that algorithmic warfare risks creating "flash conflicts" in which human oversight becomes increasingly marginal.

Beyond conventional military applications, AI also expands the analytical scope of security studies to include cyber operations and hybrid threats. Pauwels (2020) conceptualizes AI as a systemic geopolitical force that operates across economic, technological, and security domains simultaneously. ENISA's threat landscape reports confirm that AI enhances both defensive and offensive cyber capabilities, enabling automated vulnerability detection, intrusion response, and adaptive malware development (ENISA, 2021; 2023; 2025). These developments challenge existing models of deterrence, which rely on attribution and proportional response—both of which are complicated by AI-enabled cyber operations.

Security studies have also increasingly focused on the role of AI in information warfare and influence operations. Generative AI, deepfakes, and algorithmic amplification tools allow state and non-state actors to manipulate information ecosystems at scale, targeting cognitive and social vulnerabilities rather than physical assets. Europol (2023) documents the growing use of AI-generated synthetic media in political interference and disinformation campaigns. Feldstein (2019) situates these practices within a broader global trend of digital repression, where AI-enabled surveillance and manipulation technologies reinforce authoritarian control while simultaneously undermining democratic resilience.

The Russia–Ukraine war has become a central empirical reference point for contemporary security studies, demonstrating how AI-enabled systems operate in real conflict environments. Bendett (2023) shows how Russian military debates increasingly emphasize AI for command-and-control, drone coordination, and electronic warfare, while Bondar (2025) documents Ukraine's innovative integration of AI-enhanced autonomous systems, commercial satellite imagery, and real-time data analytics. These developments illustrate the fusion of state and non-state actors, military and civilian technologies, and public and private innovation ecosystems in modern warfare.

German, Moustakis, and Liaropoulos (2025) conceptualize this transformation as the co-evolution of technology and warfare, whereby strategic doctrines adapt in response to technological affordances while simultaneously shaping future innovation trajectories. From this perspective, AI does not merely enhance existing military capabilities but redefines the cognitive and organizational foundations of security practice.

Importantly, the evolution of security studies under the influence of AI also raises normative and legal questions that extend beyond operational effectiveness. The increasing reliance on algorithmic decision-support systems in both military and internal security contexts challenges assumptions about accountability, transparency, and democratic oversight. These issues necessitate closer integration between security studies, legal analysis, and political ethics—an interdisciplinary convergence that underpins the analytical approach of this thesis.

2.3 Concepts of Digital Sovereignty, Strategic Autonomy, and Human-Centric AI

The European Union's response to artificial intelligence in the security domain is structured around the interrelated concepts of digital sovereignty, strategic autonomy, and human-centric AI governance. These concepts provide the conceptual bridge between technological innovation, security imperatives, and the EU's normative identity.

Digital sovereignty refers to the capacity of political authorities to exercise effective control over digital infrastructures, data flows, and technological ecosystems within their jurisdiction. Broeders, Cristiano, and Kaminska (2023) argue that digital sovereignty has emerged as a central political objective as states seek to reduce dependency on foreign technologies and regain regulatory authority in an increasingly interconnected digital environment. For the EU, digital sovereignty is closely linked to concerns about dependence on non-European cloud providers, semiconductor supply chains, and AI platforms.

Strategic autonomy extends this logic into the security and defence domain. Fiott (2018) and Csernatoni (2021) note that the EU's pursuit of strategic autonomy reflects a gradual recalibration of its role as a security actor, moving beyond crisis management toward greater capacity for independent action. Liaropoulos (2021; 2024) emphasizes that AI constitutes a critical enabler of this ambition, as military effectiveness increasingly depends on data-driven systems, autonomous platforms, and secure digital infrastructures. Without indigenous AI capabilities, Europe risks strategic dependence on allied or rival powers, undermining both operational flexibility and political sovereignty.

The geopolitical dimension of these debates is reinforced by the global competition over AI standards and governance models. Manners' (2002) concept of Normative Power Europe remains highly relevant, as the EU continues to project influence through regulatory frameworks rather than military dominance. Bradford's (2020) analysis of the Brussels Effect demonstrates how EU regulations, including those governing AI, can shape global practices by setting de facto international standards. Smuha (2021) further conceptualizes this dynamic as a regulatory race, in which legal frameworks become instruments of geopolitical competition.

Human-centric AI constitutes the normative core of the EU's digital and security strategy. The Ethics Guidelines for Trustworthy AI articulate principles such as human agency, accountability, transparency, and technical robustness as foundational requirements for AI systems deployed within the Union (European Commission, 2019). These principles are further embedded in the Artificial Intelligence Act, which operationalizes a risk-based regulatory approach designed to protect fundamental rights while enabling innovation (European Union, 2024). UNESCO's Recommendation on

the Ethics of Artificial Intelligence reinforces this rights-based framework at the international level, strengthening the EU's normative alignment with global ethical standards (UNESCO, 2021).

At the same time, the pursuit of human-centric AI generates internal tensions. Liaropoulos (2022) warns that authoritarian models of AI governance—characterized by pervasive surveillance and political control—pose a direct challenge to liberal democratic approaches. The global diffusion of such models raises the risk of ethical externalization, whereby European technologies or standards may be applied in contexts that undermine human rights abroad.

Kapsokoli's analyses of cybersecurity governance further illustrate the institutional complexity of implementing digital sovereignty and human-centric AI in practice. She highlights the fragmentation of competencies between EU institutions and member states, which complicates coordinated responses to cyber threats and AI-enabled hybrid operations (Kapsokoli, 2020; 2021). These governance gaps risk undermining the effectiveness of the EU's regulatory ambitions unless accompanied by deeper integration and operational coordination.

The EU's emphasis on digital sovereignty and human-centric AI gains further significance when placed in a comparative geopolitical context. Competing models of AI governance reflect different assumptions about the relationship between state power, market forces, and individual rights, shaping how AI is integrated into security practices across political systems (Manners, 2002; Pauwels, 2020). In this sense, AI regulation functions not only as a domestic policy instrument but also as a strategic signal within an emerging global competition over technological norms and standards.

The European regulatory approach contrasts with more market-driven or security-centric models that prioritize rapid innovation and capability deployment. Bradford's (2020) concept of the Brussels Effect illustrates how EU regulatory standards can acquire global reach through market power rather than coercion, while Smuha (2021) characterizes this process as a form of regulatory competition in which governance capacity becomes a strategic asset. However, regulatory leadership also generates internal tensions, particularly in security contexts where speed, secrecy, and adaptability are operational imperatives. The pursuit of digital sovereignty thus involves a balancing act between normative consistency and strategic effectiveness (Broeders et al., 2023; Csernatoni, 2021).

The geopolitical dimension of AI governance reinforces the security relevance of strategic autonomy. Dependence on external suppliers for critical digital infrastructures, data ecosystems, or AI components can translate into strategic vulnerability under conditions of crisis or coercion. Liaropoulos (2021; 2024) argues that digital sovereignty is therefore inseparable from defence autonomy, as technological dependence undermines both operational effectiveness and political decision-making capacity. In this sense, AI governance becomes a core component of broader debates on European security and resilience.

At the same time, alternative governance trajectories illustrate the diversity of normative assumptions shaping AI deployment. State-centric and surveillance-oriented models demonstrate how AI-enabled systems can be used to consolidate political authority and normalize extensive monitoring practices. Liaropoulos' (2022) analysis of digital authoritarianism highlights how such models challenge liberal democratic approaches to AI governance and complicate global norm-setting efforts. These contrasts sharpen the EU's self-definition as a promoter of human-centric AI while also revealing the strategic costs associated with sustaining such a model in a competitive international environment.

Taken together, digital sovereignty, strategic autonomy, and human-centric AI form the conceptual triad underpinning the EU's approach to AI in security. They reflect an attempt to reconcile technological competitiveness with legal accountability and ethical restraint. Understanding this balance is essential for assessing the EU's capacity to respond to AI-driven security challenges without compromising its foundational values.

3. AI APPLICATIONS IN THE SECURITY SECTOR

3.1 Military and Defence Applications

Artificial intelligence has become a central driver of military transformation, reshaping how armed forces plan, conduct, and sustain operations. Contemporary military innovation increasingly revolves around data-driven systems, autonomous platforms, and algorithmic decision-making, which collectively alter the structure and tempo of warfare. Allen and Chan (2017) argue that AI should be understood not merely as a tactical enabler but as a core component of national security infrastructure, underpinning early warning systems, logistics optimization, intelligence analysis, and strategic decision support. In this sense, AI constitutes a foundational determinant of military power in the twenty-first century.

One of the most significant military applications of AI lies in intelligence, surveillance, and reconnaissance (ISR). Machine-learning algorithms process vast quantities of data derived from satellites, drones, sensors, and open-source intelligence, enabling the rapid detection of enemy movements and the identification of anomalies (Boulanin, 2019; Boulanin et al., 2020). These capabilities significantly shorten the observe–orient–decide–act (OODA) loop, allowing military forces to respond more quickly to emerging threats. Johnson (2019) emphasizes that this compression of decision-making

time fundamentally alters command dynamics and crisis stability, as human judgment is increasingly supplemented or constrained by algorithmic outputs.

AI also plays a critical role in the development of autonomous and semi-autonomous weapon systems. Boulanin and Verbruggen (2017) document the progressive automation of functions along the kill chain, from target identification to engagement. While most deployed systems remain human-in-the-loop or human-on-the-loop, operational pressures incentivize greater autonomy, particularly in environments characterized by electronic warfare, degraded communications, or high operational tempo. Proponents argue that autonomous systems may enhance precision and reduce human error, whereas critics warn that delegating lethal decision-making to algorithms raises profound legal and ethical concerns (Scharre, 2018; Sparrow, 2007).

The digitization of the battlefield extends beyond weapons platforms to human–machine integration. Liaropoulos (2023) highlights the growing use of AI-enabled augmented and virtual reality systems for training, mission rehearsal, and situational awareness. These technologies enhance cognitive performance by fusing real-time data with immersive visualization, enabling soldiers and commanders to operate more effectively in complex environments. Building on this logic, German, Moustakis, and Liaropoulos (2025) show how the co-evolution of technology and warfare materializes at the operational level, as military doctrines, force structures, and training practices adapt to AI-enabled capabilities while simultaneously shaping future patterns of defence innovation.

Within the European Union, defence-related AI development is increasingly recognized as a strategic priority. The European Defence Agency has launched several initiatives aimed at integrating AI into defence capabilities, including projects focused on automated detection, recognition, and tracking, as well as explosive device identification (European Defence Agency, 2021; 2024). Nevertheless, progress remains uneven. Liaropoulos (2024) argues that without sustained investment and coordinated procurement, Europe risks lagging behind major powers in military AI, undermining both operational effectiveness and strategic autonomy.

3.2 AI in Cybersecurity and Hybrid Threats

Artificial intelligence has fundamentally transformed the cybersecurity landscape, enhancing both defensive and offensive capabilities. On the defensive side, AI enables automated threat detection, anomaly analysis, and real-time incident response. ENISA's threat landscape reports highlight how machine-learning systems support intrusion detection, vulnerability assessment, and adaptive defence mechanisms capable of responding to evolving attack patterns (ENISA, 2021; 2023; 2025).

At the same time, adversaries increasingly weaponize AI to conduct sophisticated cyber operations. Europol (2020; 2023; 2024) documents the use of AI-enhanced phishing, automated malware development, and deep-fake-enabled fraud. Musser et al. (2023) further warn of adversarial machine learning techniques designed to deceive or corrupt AI systems through data poisoning or model manipulation, thereby undermining trust in automated security tools.

Cyber operations increasingly intersect with hybrid threats that combine digital attacks with political, economic, and informational pressure. AI plays a central role in enabling influence operations through automated content generation, micro-targeting, and algorithmic amplification. Europol (2023) reports that AI-generated synthetic media has been used to impersonate political leaders, manipulate public opinion, and destabilize democratic processes. These practices align with Feldstein's (2019) analysis of digital repression, whereby AI-enabled surveillance and manipulation technologies reinforce authoritarian control while simultaneously challenging democratic resilience.

From a governance perspective, AI-enabled hybrid threats expose structural vulnerabilities within the European security architecture. Kapsokoli (2020; 2021) highlights the fragmentation of EU cybersecurity governance, where national competencies, limited data sharing, and institutional overlap complicate coordinated responses. Attribution becomes particularly difficult when AI-assisted operations are conducted through proxies or plausibly deniable actors, undermining deterrence and the effectiveness of the EU's cyber sanctions regime.

AI also shapes internal security practices through intelligence-led policing and predictive analytics. Law enforcement agencies increasingly rely on algorithmic tools to identify risk patterns, allocate resources, and support investigative decision-making (Gkougkoudis et al., 2022). While these applications may enhance efficiency, they raise concerns regarding transparency, bias, and fundamental rights, reinforcing the need for robust oversight mechanisms (European Union Agency for Fundamental Rights, 2020; 2023).

3.3 Case Study: The Russia–Ukraine War

The Russia–Ukraine war provides the most comprehensive empirical illustration to date of AI-enabled warfare in practice. The conflict demonstrates how autonomous systems, algorithmic intelligence, and hybrid operations converge to reshape contemporary military operations. Bendett (2023) notes that Russian military discourse increasingly emphasizes AI for command-and-control, drone coordination, and electronic warfare, framing autonomy as essential for overcoming manpower constraints and operational complexity.

The most visible manifestation of AI in the conflict is the extensive use of drones. Ukrainian forces employ AI-enhanced drones for reconnaissance, artillery targeting, and strike missions. Machine-learning algorithms support autonomous navigation, object recognition, and adaptive pathfinding, particularly in environments affected by Russian electronic warfare (Bondar, 2025; ENISA, 2025). Loitering munitions used by both sides integrate varying degrees of autonomy, illustrating the gradual shift toward algorithmic targeting in high-intensity conflict.

Beyond kinetic operations, AI plays a crucial role in battlefield data fusion. Ukraine integrates commercial satellite imagery, open-source intelligence, and sensor data processed through machine-learning systems to identify troop movements and logistical nodes in near real time. This capability significantly shortens kill chains and enhances operational responsiveness, blurring the boundary between civilian and military technological ecosystems.

The war also highlights the vulnerabilities of AI-enabled systems. Both sides have targeted drones and autonomous platforms through electronic warfare, spoofing, and cyber interference, demonstrating that autonomy remains deeply dependent on resilient digital infrastructures. ENISA (2025) emphasizes that these interactions underscore the necessity of integrated cyber–AI defence strategies, particularly for European armed forces that rely on networked systems.

AI has further been deployed in information warfare. Early in the conflict, AI-generated deepfake videos falsely depicting Ukrainian political leaders announcing surrender were disseminated online, illustrating the use of synthetic media to undermine morale and manipulate perceptions (Europol, 2023). These operations demonstrate how AI-enabled influence campaigns operate alongside kinetic warfare, reinforcing the hybrid nature of contemporary conflict.

While the Russia–Ukraine war illustrates the operational relevance of AI-enabled systems, it also exposes important constraints that qualify narratives of technological determinism. AI-supported capabilities remain deeply dependent on contested infrastructures, including communications networks, satellite navigation, data integrity, and organizational integration. In an environment characterized by electronic warfare, deception, and rapid adaptation, these dependencies significantly shape operational outcomes (Horowitz & Scharre, 2021; Johnson, 2019). Autonomy does not eliminate vulnerability; rather, it redistributes it across digital and informational layers that can be targeted by adversaries.

Drone warfare provides a particularly revealing example. Although drones have transformed reconnaissance, targeting, and strike coordination, they remain highly susceptible to jamming, spoofing, and interception. AI-assisted navigation and targeting depend on signal reliability and sensor accuracy, both of which are actively contested in the conflict. ENISA's threat assessments highlight how AI-enabled systems can attack surfaces themselves, particularly when adversaries exploit data dependencies or model weaknesses (ENISA, 2023; ENISA, 2025). The resulting cycle of adaptation

underscores that technological advantage in AI-enabled warfare is often temporary rather than decisive.

The conflict also underscores the organizational dimension of AI integration. Algorithmic outputs must be interpreted, trusted, and acted upon by human operators under conditions of stress and uncertainty. Faster decision cycles can generate tactical advantage, but they can also amplify errors when informational inputs are incomplete or manipulated. Horowitz and Scharre (2021) warn that AI-enabled acceleration may increase escalation risks when systems interact under uncertainty, a concern that is particularly relevant in dense operational environments where multiple autonomous or semi-autonomous platforms operate simultaneously.

From a European perspective, war provides critical lessons for defence planning and strategic autonomy. Effective use of AI-enabled systems in Ukraine has often relied on civilian technologies, commercial platforms, and flexible innovation networks. Bondar (2025) notes that this approach enhances adaptability but also raises sustainability and dependency concerns. Reliance on non-European platforms and supply chains can translate into strategic vulnerability if access is disrupted or politically conditioned, reinforcing arguments that strategic autonomy in AI is a practical requirement rather than an abstract policy goal (Csernatoni, 2021; Liaropoulos, 2024).

Finally, the conflict highlights the importance of resilience and integration across domains. AI-enabled military capabilities cannot be isolated from cybersecurity, hybrid threat response, and information integrity. Attacks on data, networks, and public trust can undermine the effectiveness of even advanced systems, reinforcing the need for integrated European approaches that link defence innovation with cyber resilience and institutional coordination (Kapsokoli, 2020; ENISA, 2023).

For Europe, the Russia–Ukraine war has strategic implications. Csernatoni (2024) argues that the conflict exposed critical gaps in European defence capabilities, particularly in drone production, counter-drone systems, and rapid innovation cycles. Liaropoulos (2024) similarly notes that the war underscores the urgency of investing in military AI as a prerequisite for credible European strategic autonomy.

3.4 AI, Hybrid Warfare, and Influence Operations

Artificial intelligence amplifies the complexity, reach, and ambiguity of hybrid warfare. Influence operations increasingly rely on generative AI, deepfakes, and algorithmic targeting to manipulate information ecosystems at scale. These tools enable adversaries to tailor narratives to specific audiences, exploit emotional triggers, and overwhelm fact-checking mechanisms (Europol, 2023; ENISA, 2023).

Pauwels (2020) conceptualizes AI-enabled influence as a form of geopolitical competition over cognitive space, where power is exercised through perception management rather than direct coercion. In this context, algorithmic influence becomes a strategic instrument operating below the threshold of armed conflict while producing tangible security effects. Liaropoulos (2022) similarly warns that digital authoritarian regimes leverage AI to extend political control domestically and project influence externally.

The European Union faces particular challenges in this domain due to the openness of its information environment. While Bradford's (2020) Brussels Effect demonstrates the EU's capacity to shape global regulatory norms, this normative openness simultaneously exposes European societies to external manipulation. Kapsokoli (2023) notes that AI-enabled hybrid threats exploit legal and institutional gaps, complicating attribution and coordinated response.

These dynamics blur the traditional distinctions between war and peace, as well as external and internal security. As AI-enabled influence operations increasingly target civilian populations, democratic institutions, and public trust, they challenge conventional security frameworks and demand more integrated policy responses at the European level.

3.5 Integrating the Contributions of Liaropoulos and Kapsokoli

The works of Liaropoulos and Kapsokoli provide critical analytical lenses for understanding AI's role in European security. Liaropoulos (2021; 2023; 2024) consistently frames AI as both a strategic enabler and a source of vulnerability, central to debates on digital sovereignty and strategic autonomy. He argues that without control over AI infrastructures, data governance, and defence innovation, Europe risks strategic dependence on external actors.

Kapsokoli's scholarship complements this perspective by emphasizing governance challenges. Her analyses of cybersecurity governance and cyber sanctions highlight the fragmentation of EU competencies and the difficulty of coordinating responses to AI-enabled threats (Kapsokoli, 2020; 2021; 2023). Together, these contributions illustrate how AI reshapes not only military capabilities but also institutional and political dynamics within the EU.

3.6 AI and European Defence Capability Gaps

Artificial intelligence exposes structural gaps in European defence capabilities. The European Defence Agency acknowledges deficits in autonomous systems, counter-drone technologies, AI-enabled command-and-control, and secure defence cloud infrastructures (European Defence Agency, 2024). These gaps undermine the operational credibility of Common Security and Defence Policy missions in increasingly AI-driven environments (Panfil, Molnár, and Paile-Calvo).

Comparative analysis further highlights Europe's relative lag. Kania (2017) demonstrates how China's military–civil fusion strategy accelerates AI integration by leveraging commercial innovation at scale. By contrast, Europe's fragmented defence-industrial base and regulatory caution slow deployment. German, Moustakis, and Liaropoulos (2025) argue that this divergence reflects different co-evolutionary pathways between technology and warfare.

Liaropoulos (2024) warns that unless the EU overcomes these structural and institutional constraints, strategic autonomy risks remain declaratory rather than operational. Kapsokoli (2020; 2021) similarly emphasizes that cybersecurity fragmentation compounds technological gaps, as AI-enabled defence systems require harmonized digital infrastructures and shared standards.

The Russia–Ukraine war has intensified pressure on the EU to address these shortcomings. ENISA (2025) notes that AI-enabled cyber operations, drone warfare, and hybrid threats demand integrated investment, doctrinal alignment, and civil–military coordination. Closing Europe's AI capability gap thus constitutes a central challenge for its future security posture.

4. LEGAL IMPLICATIONS

4.1 International Humanitarian Law and Lethal Autonomous Weapons

The increasing integration of artificial intelligence into military systems presents a qualitative challenge to international humanitarian law rather than a simple extension of existing weapons technologies. IHL regulates the conduct of hostilities through core principles such as distinction, proportionality, precautions in attack, and accountability for the use of force. These principles presuppose the application of human judgment in context-sensitive targeting decisions and the ability to attribute responsibility through identifiable chains of command. The delegation of target selection or engagement functions to autonomous or semi-autonomous systems places these assumptions under significant strain (Schmitt & Thurnher, 2013; Boulanin & Verbruggen, 2017).

The principle of distinction is particularly affected by AI-enabled targeting. Distinction requires the differentiation of combatants and military objectives from civilians and

civilian objects in dynamic and often ambiguous environments. Machine-learning systems operate through probabilistic pattern recognition based on training data that may be incomplete, biased, or poorly suited to rapidly changing battlefield contexts. Boulanin (2019) and Boulanin et al. (2020) emphasize that even highly accurate systems may struggle to interpret intent, surrender, or civilian presence in ways that satisfy legal standards, especially where visual or behavioral cues are context-dependent.

Proportionality raises an even deeper legal challenge. Proportionality assessments require a qualitative balancing between anticipated military advantage and expected incidental civilian harm. This balancing is inherently normative and cannot be reduced to numerical thresholds or damage estimates alone. Roff and Moyes (2016) argue that while AI systems may assist in estimating effects, they cannot replace the evaluative judgment required to determine whether harm would be excessive under IHL. For this reason, debates surrounding "meaningful human control" focus not merely on the presence of human involvement, but on whether humans remain positioned at the point of normative judgment rather than relegated to supervisory or post hoc roles.

The obligation to take feasible precautions in attack further illustrates the tension between autonomy and legal responsibility. Precautions require verification of targets and the selection of means and methods designed to minimize civilian harm. As autonomy increases and operational tempo accelerates, opportunities for human verification may diminish, particularly in environments characterized by degraded communications or electronic warfare. Scharre (2018) notes that increased reliance on autonomous functions risks normalizing pre-delegated authority to use force, thereby weakening the precautionary logic embedded in IHL.

These challenges have been the subject of sustained debate within the framework of the Convention on Certain Conventional Weapons. Since 2017, the Group of Governmental Experts on lethal autonomous weapons systems has examined whether existing law is sufficient or whether new legally binding instruments are required. While states have endorsed guiding principles emphasizing human responsibility, consensus on prohibition or regulation remains elusive, reflecting divergent strategic interests and perceptions of military advantage (United Nations, 2019; United Nations Convention on Certain Conventional Weapons, 2017–2025).

Against this backdrop, the International Committee of the Red Cross has articulated a more restrictive position. The ICRC has called for clear prohibitions on autonomous weapons that are unpredictable or designed to target humans without meaningful human control, alongside limits on other autonomous systems (International Committee of the Red Cross, 2021). This approach reflects a humanitarian interpretation of IHL that prioritizes civilian protection and accountability over technological flexibility. Parallel arguments advanced by civil society organizations and scholars emphasize that delegating lethal decision-making to machines risks eroding the moral foundations of the law of armed conflict (Docherty et al., 2012; Sparrow, 2007; Campaign to Stop Killer Robots, 2018–2025).

Accountability remains a central unresolved issue. When an autonomous system causes unlawful harm, responsibility may be distributed across commanders, operators, programmers, and institutions involved in design and deployment. Matthias's (2004) concept of the "responsibility gap" captures this difficulty, particularly in relation to learning systems whose behavior may not be fully foreseeable. While IHL does not demand perfect foresight, it requires that those who decide to employ force do so on the basis of reasonable assessments consistent with legal duties. The deployment of systems whose outcomes cannot be sufficiently anticipated, therefore, raises fundamental questions about compatibility with IHL's accountability structure (Schmitt & Thurnher, 2013; Roff & Moyes, 2016).

Within the European Union, these legal concerns are reflected in repeated institutional statements emphasizing the necessity of meaningful human control and the primacy of humanitarian and human rights considerations. The European Parliament has consistently supported stronger international regulation of autonomous weapons and framed autonomy as a normative boundary rather than a purely technical parameter (European Parliament, 2018; 2023). This position aligns with the EU's broader commitment to human-centric AI governance, even as military applications remain largely outside the scope of civilian AI regulation (European Union, 2024; Liaropoulos, 2024).

4.2 Human Rights Law and AI in Security Contexts

Outside situations of armed conflict, the legality of AI in security is primarily shaped by international and European human rights law. AI systems are increasingly deployed in policing, border management, intelligence analysis, and surveillance, expanding state capacity to process personal data, infer behavior, and make risk-based decisions. While such systems may enhance efficiency and situational awareness, they also amplify the risk of unlawful interference with fundamental rights if safeguards, transparency, and oversight are insufficient (European Union Agency for Fundamental Rights, 2020; 2023).

Privacy and data protection constitute the core legal concerns in this domain. Solove's (2006) taxonomy of privacy clarifies that harm arises not only from surveillance itself but from aggregation, profiling, secondary use, and the exclusion of individuals from meaningful knowledge or control over data processing. AI systems intensify these risks by enabling continuous inference across datasets and contexts, often producing probabilistic judgments that are difficult to contest. In the EU legal order, the General Data Protection Regulation establishes the baseline requirements governing such processing, including lawfulness, purpose limitation, data minimization, transparency, and security (European Union, 2016).

Particularly relevant for security uses of AI is the GDPR's restriction on certain forms of solely automated decision-making that produce legal or similarly significant effects. In areas such as policing, migration control, or criminal justice, algorithmic systems may substantially shape decisions affecting liberty, access to services, or legal status. Iglezakis (2021) emphasizes that safeguards in this context must ensure genuine contestability and human intervention, rather than formal compliance without substantive protection.

Biometric surveillance represents one of the most sensitive applications of AI in security contexts. Facial recognition and other biometric identification technologies raise acute concerns about mass surveillance, chilling effects, and the erosion of anonymity in public spaces. The Clearview AI case demonstrates how biometric data processing without legal basis can trigger significant enforcement action under European data protection law (Hellenic Data Protection Authority, 2022; Homo Digitalis, 2022). The broader concern is not limited to individual consent but relates to the structural impact of biometric surveillance on democratic life and freedom of assembly (European Union Agency for Fundamental Rights, 2020).

Non-discrimination and equality law further constrain AI use in security. The FRA warns that biased training data and proxy variables can generate indirect discrimination, particularly in predictive policing and risk assessment systems, where feedback loops may reinforce existing inequalities (European Union Agency for Fundamental Rights, 2023). Recognizing these risks, the European Parliament has called for strict safeguards when AI is used by police and judicial authorities, stressing proportionality, necessity, and accountability (European Parliament, 2021).

Human rights analysis must also address the tendency of security rationales to normalize exceptional measures. While public safety objectives may justify certain limitations on rights, European human rights law requires that any such limitations be grounded in clear legal bases, demonstrate genuine necessity, and remain proportionate to the security aim pursued. AI's scalability and opacity risk transforming surveillance and profiling into routine practices rather than exceptional responses. Saheb (2023) highlights how AI-enabled surveillance reshapes power relations between citizens and the state, producing chilling effects that are legally relevant insofar as they undermine the effective enjoyment of rights.

Finally, the transnational diffusion of security technologies raises questions of indirect responsibility. Feldstein (2019) and Liaropoulos (2022) show how AI-enabled surveillance and control tools facilitate digital repression in authoritarian contexts. When democratic jurisdictions develop, export, or support such technologies, they face growing expectations of human-rights-based due diligence, reinforcing the link between internal governance standards and external responsibility.

4.3 European Union Law and the Artificial Intelligence Act (2024)

The European Union has developed a distinctive legal approach to artificial intelligence that combines market harmonization, rights protection, and risk-based governance. This approach is reflected in the GDPR, the Cybersecurity Act, and most prominently in the Artificial Intelligence Act adopted in 2024 (European Union, 2016; 2019; 2024). Together, these instruments seek to provide legal certainty while constraining harmful uses of AI and structuring accountability across the AI lifecycle.

The AI Act establishes a tiered framework based on risk classification, attaching differentiated obligations to unacceptable-risk, high-risk, limited-risk, and minimal-risk systems. This structure operationalizes the EU's human-centric AI philosophy, articulated earlier in the Ethics Guidelines for Trustworthy AI, which emphasize human agency, accountability, transparency, and technical robustness (European Commission, 2019). For high-risk systems, the Act imposes requirements related to data governance, documentation, human oversight, cybersecurity, and post-market monitoring (European Union, 2024).

Security-related applications occupy a central position within this framework. AI systems used in law enforcement, migration and border control, and the administration of justice are classified as high risk, reflecting recognition that such systems intensify state coercive power and pose heightened risks to fundamental rights. Oversight institutions have emphasized that the effectiveness of this framework depends on robust enforcement. The EDPB and EDPS have repeatedly warned against overly permissive interpretations, particularly in relation to biometric surveillance and law enforcement exemptions (European Data Protection Board & European Data Protection Supervisor, 2021; European Data Protection Supervisor, 2023).

Academic critique reinforces these concerns. Veale and Zuiderveen Borgesius (2021) argue that risk-based regulation can suffer from ambiguity regarding classification, scope, and enforcement, especially where systems evolve after deployment or where purposes expand over time. These issues are particularly salient in security environments, where operational imperatives may encourage function creep unless legal constraints are actively enforced.

The governance significance of the AI Act in security contexts lies not only in its formal classification system but in how its obligations interact with operational realities. Security institutions operate under conditions of urgency, secrecy, and asymmetric threats, complicating the implementation of transparency, explainability, and oversight requirements. While the Act seeks to strengthen accountability, there is a risk that compliance becomes procedural rather than substantive if documentation and human-oversight mechanisms do not translate into effective scrutiny (Veale & Zuiderveen Borgesius, 2021; European Data Protection Supervisor, 2023).

Implementation challenges are particularly acute in law enforcement and border management, where AI systems may evolve after deployment and be repurposed across

agencies. Risk-based regulation struggles with such fluidity, especially when systems continue learning or are integrated into broader surveillance architectures. This raises concerns about function creep and long-term proportionality, as systems initially justified for narrow purposes may gradually expand in scope without equivalent reassessment of rights impacts (European Union Agency for Fundamental Rights, 2023; Solove, 2006).

Enforcement capacity further shapes the Act's effectiveness. Oversight depends on national authorities' technical expertise, resources, and institutional independence. Variations across member states may result in uneven application, particularly in security-sensitive domains where political pressure and operational discretion are pronounced. Smuha (2021) emphasizes that regulatory ambition must be matched by institutional capability if governance frameworks are to remain credible in practice.

Finally, the AI Act brings into focus the structural boundary between civilian and military governance. While military AI remains largely excluded from its scope, civilian and internal security applications are subject to extensive obligations. This asymmetry risks producing parallel governance regimes, even though the most severe ethical and legal risks may arise precisely in defence contexts. Liaropoulos (2024) argues that this tension reflects a broader European dilemma: reconciling regulatory leadership and normative power with the pursuit of strategic autonomy in an increasingly competitive security environment. `

The AI Act must also be understood within a broader geopolitical context. Smuha (2021) conceptualizes AI regulation as a form of regulatory competition, where legal frameworks themselves become instruments of strategic influence. Bradford's (2020) Brussels Effect further explains how EU regulation can shape global practices through market power. However, in security and defence, these dynamics are more complex, as military AI often falls outside standard market logics and remains closely tied to national sovereignty.

A key structural limitation of the EU framework lies in the separation between civilian AI regulation and military applications. The AI Act does not comprehensively regulate military AI used in armed conflict, reflecting competence boundaries and political sensitivity (European Union, 2024). This creates an asymmetry in governance: stringent oversight for many internal security uses coexists with more fragmented regulation of military autonomy, despite the severity of associated legal risks. Liaropoulos (2024) identifies this gap as a central challenge for reconciling European strategic autonomy with ethical and legal leadership.

Cybersecurity and robustness further complicate legal governance. AI systems are vulnerable to adversarial manipulation, data poisoning, and exploitation of model weaknesses. Legal requirements of safety and robustness, therefore, intersect with technical resilience. Nolte et al. (2025) highlight the importance of cybersecurity obligations within the AI Act, while ENISA's threat landscape reports demonstrate that AI systems can simultaneously function as security tools and attack surfaces (ENISA,

2023; 2025). For security actors, legal compliance cannot be separated from technical integrity.

Taken together, EU law establishes a rights-oriented and risk-based model of AI governance with global ambition yet marked by important boundaries when confronted with military autonomy and rapidly evolving threat environments. These tensions provide the foundation for the ethical analysis developed in the following chapter, particularly regarding responsibility, meaningful human control, and the diffusion of ethically contentious security technologies.

5. ETHICAL IMPLICATIONS AND GOVERNANCE CHALLENGES

5.1 Accountability and the "Responsibility Gap"

One of the most persistent ethical challenges raised by artificial intelligence in the security domain concerns accountability. While legal frameworks focus on attribution of responsibility and compliance with formal rules, ethical analysis interrogates whether responsibility remains meaningful when decision-making processes are increasingly delegated to autonomous or learning systems. This concern is commonly conceptualized as the "responsibility gap," a term introduced by Matthias (2004) to describe situations in which outcomes produced by autonomous systems cannot be fully traced back to any single human agent.

In security contexts, the responsibility gap is not merely hypothetical. AI systems are often embedded within complex socio-technical assemblages involving designers, data curators, military planners, commanders, operators, and political authorities. As machine-learning systems adapt over time, their behavior may diverge from initial design intentions, making it difficult to foresee specific outcomes. Ethically, this raises questions about moral agency: if no human can reasonably predict or control a system's behavior, it becomes unclear who ought to bear moral blame when harm occurs (Sparrow, 2007).

This challenge is particularly acute in military and policing applications, where AI-supported decisions may involve the use of force, deprivation of liberty, or long-term social consequences. Kaspersen and Taddeo (2021) argue that accountability in defence AI must be understood as a distributed responsibility that extends beyond immediate operators to institutional and political decision-makers. Ethical responsibility thus cannot be discharged merely by maintaining nominal human oversight; it requires meaningful governance structures that allocate responsibility across the entire lifecycle of AI systems.

From a European perspective, the responsibility gap intersects with democratic accountability. The delegation of decision-making authority to opaque systems risks weakening public oversight and political responsibility, particularly where security decisions are shielded by secrecy or technical complexity. Sampathianaki (2025) emphasizes that AI governance in democratic societies must preserve the ability of citizens to hold institutions accountable, even when decisions are mediated by complex technologies. Without such safeguards, AI risks eroding the ethical foundations of democratic security governance.

5.2 Meaningful Human Control over Lethal Systems

The concept of meaningful human control has emerged as a central ethical principle in debates over autonomous weapons and AI-enabled security systems. While the concept has legal relevance, its ethical significance lies in its attempt to preserve human moral agency in decisions involving harm. Meaningful human control requires more than formal human involvement; it demands that humans retain substantive understanding, authority, and the ability to intervene in critical functions (Roff & Moyes, 2016).

Ethically, the insistence on meaningful human control reflects the belief that decisions to use force against human beings should not be delegated entirely to machines. Sparrow (2007) argues that allowing machines to make lethal decisions risks undermining human dignity by treating individuals as objects of algorithmic optimization rather than moral subjects. Sharkey (2012; 2018) similarly contends that removing humans from the decision loop risks normalizing violence and diluting moral responsibility.

The challenge, however, lies in operationalizing meaningful human control in high-speed, AI-driven environments. As autonomous systems operate at machine speed, human intervention may become impractical or illusory. Scharre (2018) notes that in such contexts, human oversight may be reduced to pre-programming and post hoc review rather than real-time moral judgment. Ethically, this raises the question of whether control exercised ex ante can substitute for control exercised at the moment of action.

The European Union has consistently endorsed meaningful human control as an ethical and political commitment. European Parliament resolutions and EEAS positions frame human control not only as a safeguard against harm but as an expression of European values in warfare and security governance (European Parliament, 2018; EEAS, 2024). Liaropoulos (2024) observes that this normative stance places Europe in a difficult position: while advocating restraint and ethical leadership, the EU must simultaneously

ensure that its armed forces remain operationally credible in an environment where autonomy is increasingly normalized by other powers.

Thus, meaningful human control functions as both an ethical boundary and a governance challenge. Its ethical value is clear, but its practical realization requires institutional design choices, training doctrines, and technological architectures that prioritize human judgment rather than marginalizing it.

5.3 Digital Authoritarianism and Ethical Risk Exportation

Beyond individual systems, AI in security raises broader ethical questions about global power, governance models, and the diffusion of norms. One of the most significant developments in this regard is the rise of digital authoritarianism, understood as the use of AI-enabled technologies for pervasive surveillance, behavioral control, and political repression. Feldstein (2019) documents how authoritarian regimes deploy AI to monitor populations, suppress dissent, and manipulate information environments at an unprecedented scale.

Liaropoulos (2022) further demonstrates how digital authoritarian practices are increasingly exported through technology transfer, infrastructure projects, and security cooperation. AI-enabled surveillance systems, biometric databases, and predictive policing tools developed in one political context may be deployed in another with vastly different human rights standards. This raises ethical concerns about complicity and responsibility, particularly for democratic actors involved in the development, sale, or support of such technologies.

The concept of ethical risk exportation captures this dynamic. Even if AI systems are developed and regulated according to ethical standards within the EU, their deployment abroad may contribute to repression if safeguards are absent or ignored. As Liaropoulos (2022) and Feldstein (2019) highlight, competing governance models—liberal democratic, authoritarian, and hybrid—vie for legitimacy in the global AI order. Ethical governance therefore cannot be understood solely as a domestic issue; it has transnational implications.

From an ethical standpoint, this challenges the EU's self-conception as a normative power. Manners (2002) argues that normative influence depends not only on rule-making but on consistency between internal values and external practices. If European

actors contribute to the spread of ethically contentious security technologies, the credibility of human-centric AI governance may be undermined.

UNESCO's Recommendation on the Ethics of Artificial Intelligence provides a global ethical framework that addresses these concerns by emphasizing human rights, cultural diversity, and international cooperation (UNESCO, 2021). However, translating such principles into enforceable practices remains difficult, particularly in security markets characterized by secrecy, strategic competition, and geopolitical rivalry.

5.4 Governance Challenges and Ethical Oversight

Ethical challenges surrounding AI in security are ultimately governance challenges. Ethical principles such as accountability, human control, and respect for human rights require institutional mechanisms to be effective. Floridi and Cowls (2019) argue that ethical AI governance must move beyond abstract principles toward enforceable standards, oversight bodies, and continuous evaluation.

A recurring concern is the risk of "ethics washing," where ethical guidelines are adopted rhetorically without meaningful implementation. Yeung, Howes, and Pogrebna (2020) warn that voluntary ethics frameworks, if not accompanied by legal obligations and institutional oversight, may legitimize harmful practices rather than constrain them. This risk is particularly acute in security contexts, where claims of necessity and secrecy can shield AI deployment from scrutiny.

Within the EU, governance challenges are compounded by institutional fragmentation. Civilian AI governance is relatively advanced, while defence and security applications remain subject to national discretion and limited transparency. Kapsokoli (2020; 2021) highlights how fragmented competencies in cybersecurity and defence complicate coherent ethical oversight, especially for cross-border or hybrid threats.

Ethical governance also requires interdisciplinary expertise. Evaluating AI systems in security contexts demands not only technical knowledge but legal, ethical, and strategic understanding. The lack of such integrated oversight structures increases the risk that ethical considerations will be subordinated to operational imperatives.

Ultimately, ethical governance of AI in security is not about eliminating risk but about managing it in a way consistent with democratic values and human dignity. As AI

becomes increasingly embedded in security practices, ethical oversight must evolve from an aspirational discourse into a core component of security governance.

6. THE EUROPEAN UNION'S STRATEGIC AND POLICY RESPONSE

6.1 EU Strategic Autonomy and Defence Initiatives

The growing integration of artificial intelligence into security and defence has intensified long-standing debates within the European Union regarding strategic autonomy. In this context, strategic autonomy refers to the EU's capacity to act independently in security and defence matters while maintaining cooperative relations with allies. As Fiott (2018) and Csernatoni (2021) note, concerns about dependence on external technological providers have increasingly been framed as sources of strategic vulnerability, with implications for both operational effectiveness and political decision-making.

Liaropoulos (2024) argues that military artificial intelligence has emerged as a decisive enabler of European strategic autonomy. Dependence on non-European technologies, particularly in cloud computing, data analytics, semiconductors, and AI software, creates vulnerabilities that extend beyond operational constraints to political leverage. From this perspective, AI is not merely a technological asset but a strategic prerequisite for credible defence cooperation and independent decision-making within the EU.

EU defence initiatives increasingly reflect this awareness. The European Defence Agency has placed AI at the center of its innovation agenda, supporting collaborative projects focused on automated detection, tracking, decision support, and explosive threat identification (European Defence Agency, 2021; 2024). These initiatives aim to reduce fragmentation in defence research and promote interoperability among member states. However, as Csernatoni (2021) notes, the EU's defence technological ambitions remain constrained by uneven national investment, divergent threat perceptions, and the absence of a fully integrated defence industrial base.

The tension between ambition and capacity is further shaped by the EU's reliance on partnerships, particularly with NATO and the United States. While strategic autonomy does not imply strategic isolation, the growing centrality of AI raises questions about the balance between interoperability and dependency. Liaropoulos (2021) emphasizes that digital sovereignty in defence requires not only regulatory frameworks but sustained investment in indigenous technological ecosystems capable of supporting long-term military innovation.

6.2 AI and Security in the Strategic Compass (2022)

The Strategic Compass for Security and Defence, adopted in 2022, represents the EU's most comprehensive attempt to articulate a shared strategic vision in an increasingly contested security environment. Although the document does not focus exclusively on artificial intelligence, it explicitly acknowledges the transformative impact of emerging and disruptive technologies, including AI, on future conflict and security dynamics (European External Action Service, 2022).

Within the Strategic Compass, AI is framed primarily as an enabler of situational awareness, resilience, and operational effectiveness. The document highlights the need to enhance intelligence capabilities, improve early warning mechanisms, and strengthen cyber and space security—all domains in which AI plays a critical role. This reflects a pragmatic recognition that technological superiority increasingly shapes the ability to anticipate and manage crises.

At the same time, the Strategic Compass situates AI within a values-based framework. It emphasizes that capability development must remain consistent with international law and EU values, reinforcing the Union's commitment to human-centric and responsible use of emerging technologies. This dual emphasis mirrors the broader tension identified throughout this thesis: the EU seeks to strengthen its security posture while maintaining ethical and legal restraint.

Kapsokoli (2020) observes that strategic documents such as the Compass often function as coordination tools rather than operational blueprints. Their effectiveness depends on translation into concrete capabilities, funding mechanisms, and institutional practices. In the case of AI, this translation remains uneven, as member states retain primary responsibility for defence procurement and operational deployment.

6.3 Civil–Military Research Divide in EU AI Governance

A persistent challenge in the EU's AI strategy is the divide between civilian and military research and governance frameworks. Civilian AI governance is well-developed, characterized by comprehensive regulation, clear ethical guidelines, and robust institutional oversight. Defence-related AI, by contrast, remains governed primarily at the national level, with limited transparency and coordination at the EU level.

This divide reflects both legal competence boundaries and political sensitivity surrounding defence. However, it also produces practical consequences. Many AI technologies relevant to security—such as machine learning, computer vision, and data analytics—are inherently dual-use. Separating civilian and military research can therefore slow innovation, complicate technology transfer, and reduce economies of scale.

Liaropoulos (2024) argues that overcoming this divide is essential for European strategic autonomy. Without closer integration between civilian innovation ecosystems and defence requirements, the EU risks falling behind actors that pursue more integrated civil–military approaches to AI development. At the same time, integration raises governance challenges, as civilian oversight mechanisms may not automatically extend to military applications.

Kapsokoli's analysis of cybersecurity governance highlights similar structural tensions. She notes that fragmented governance across policy domains complicates coherent responses to hybrid and AI-enabled threats, particularly when coordination depends on voluntary cooperation rather than binding mechanisms (Kapsokoli, 2020; 2021). In this sense, the civil–military divide is not merely institutional but reflects broader questions about sovereignty, trust, and accountability within the EU.

6.4 Policy Gaps and Coordination Challenges

Despite significant progress in articulating strategic objectives and regulatory frameworks, gaps remain in the EU's AI security posture. One such gap concerns coordination between regulatory ambition and operational capability. While the EU has positioned itself as a global leader in AI governance, its ability to translate norms into security-relevant capabilities remains uneven.

Coordination challenges are particularly evident in areas such as defence procurement, data sharing, and operational interoperability. The absence of common standards for military AI, coupled with national procurement priorities, limits the scalability of EU initiatives. Panfil, Molnár, and Paile-Calvo note that Common Security and Defence Policy missions increasingly operate in environments shaped by digital and AI-enabled threats yet lack unified technological frameworks to address them effectively.

Another policy gap concerns crisis responsiveness. AI-enabled threats evolve rapidly, often below the threshold of armed conflict. EU decision-making processes, by contrast, are frequently slow and consensus-driven. This mismatch risks undermining the Union's ability to respond effectively to hybrid threats, cyber incidents, and influence operations. Kapsokoli (2021) highlights that while instruments such as cyber sanctions exist, their effectiveness depends on attribution and political consensus, both of which are challenged by AI-enabled ambiguity.

Finally, the EU faces a strategic dilemma between openness and resilience. Its commitment to openness, market integration, and fundamental rights constitutes a core strength, but it also creates exposure to external manipulation and technological dependency. Addressing this dilemma requires not only regulatory measures but sustained investment, institutional learning, and political coordination.

Taken together, these gaps do not indicate the absence of strategy, but rather the complexity of aligning values, capabilities, and governance in a rapidly evolving technological environment. AI magnifies existing structural challenges within the EU's

security architecture, making coordination and integration central issues for the Union's future role as a security actor.

7. CONCLUSIONS AND POLICY RECOMMENDATIONS

7.1 Summary of Findings

This thesis has examined the application of artificial intelligence in the security field through a multidisciplinary lens combining international and European security studies, legal analysis, and political ethics. It has demonstrated that AI is not merely a technological innovation but a structural force reshaping the conduct of warfare, internal security practices, and the governance of risk at both national and supranational levels. Across military, cyber, and hybrid domains, AI accelerates decision-making, expands surveillance capacity, and introduces new forms of autonomy that challenge established legal and ethical frameworks.

From a theoretical perspective, the analysis has shown that realism, liberalism, and constructivism offer complementary insights into the security implications of AI. Realist approaches illuminate the role of AI in strategic competition and power projection, liberal perspectives emphasize the importance of institutional governance and regulatory coordination, and constructivist analysis highlights the normative contestation surrounding human-centric AI and technological legitimacy. Together, these frameworks help explain why AI simultaneously functions as a strategic asset, a governance challenge, and a normative battleground in contemporary security politics.

Empirically, the examination of AI applications in military operations, cybersecurity, law enforcement, and hybrid warfare has illustrated the breadth and depth of AI's impact on security practice. The case study of the Russia–Ukraine war demonstrated how AI-enabled drones, intelligence systems, cyber operations, and influence campaigns shape modern conflict, while also exposing the vulnerabilities, escalation risks, and dependencies associated with algorithmic warfare. These findings underline

that AI does not eliminate uncertainty in security environments but redistributes it across digital, organizational, and informational domains.

At the European level, the analysis highlighted a growing gap between regulatory ambition and operational capability. While the EU has positioned itself as a global leader in ethical and legal AI governance, its defence-related AI capabilities remain uneven and fragmented. This tension lies at the heart of Europe's struggle to reconcile strategic autonomy with its normative commitments.

7.2 Legal and Ethical Takeaways

The legal analysis conducted in this thesis underscores the growing tension between existing legal frameworks and emerging AI-enabled security practices. International humanitarian law remains grounded in principles of distinction, proportionality, and accountability that presuppose meaningful human judgment. The increasing autonomy of weapons systems and decision-support tools complicates the attribution of responsibility and challenges the capacity of legal norms to regulate harm effectively in high-speed, data-driven operational contexts.

Similarly, human rights law faces mounting pressure as AI systems are deployed in policing, border management, surveillance, and predictive security. While public safety considerations may justify certain limitations on rights, such restrictions must remain lawful, necessary, and proportionate. The risk of function creep, opaque decision-making, and discriminatory outcomes highlights the importance of robust safeguards, oversight mechanisms, and accountability structures, particularly within democratic societies.

Ethically, the analysis confirms that AI in security intensifies longstanding concerns about the responsibility gap and the erosion of meaningful human control. As autonomous and semi-autonomous systems assume greater roles in security decision-making, ensuring human agency, moral accountability, and ethical restraint becomes increasingly complex. The spread of digital authoritarian practices further illustrates how AI can be instrumentalized to normalize extensive surveillance and political control, raising concerns about the externalization of ethically contentious practices beyond Europe's borders.

Together, these findings underscore the need for governance approaches that integrate legal accountability with ethical reflection, rather than treating them as separate domains.

7.3 Strategic and Policy Recommendations

On the basis of these findings, several strategic and policy-oriented conclusions emerge. First, the European Union should continue to strengthen its regulatory leadership in AI governance while ensuring that legal frameworks remain responsive to the specific challenges of security applications. The implementation of the Artificial Intelligence Act should be accompanied by sustained investment in enforcement capacity, technical expertise, and inter-agency coordination to prevent regulatory fragmentation.

Second, the pursuit of strategic autonomy in AI should be understood not as technological isolation but as a means of reducing critical dependencies and enhancing resilience. Greater investment in collaborative defence research, interoperability, and trusted innovation ecosystems is necessary to ensure that Europe can deploy AI-enabled capabilities without undermining its normative commitments.

Third, civil–military coordination must be improved to avoid the emergence of parallel governance regimes. While legal distinctions between civilian and military domains are unavoidable, greater dialogue and alignment are needed to ensure that human-centric principles inform AI development across the security spectrum. This includes engagement with international partners and multilateral fora to promote shared standards and confidence-building measures.

Finally, ethical governance should be treated as a strategic asset rather than a constraint. Embedding ethical considerations institutionally—through strengthened oversight mechanisms, interdisciplinary expertise, and integration across the AI lifecycle—can reinforce the EU's legitimacy and normative influence while mitigating the long-term risks associated with unchecked technological deployment.

7.4 Reflections on Future Research

This thesis has sought to provide a comprehensive assessment of the legal, ethical, and strategic implications of artificial intelligence in the security field. Nevertheless, it captures only a snapshot of a rapidly evolving technological and geopolitical landscape. As AI continues to advance and diffuse across security domains, scholarly analysis must

remain attentive to both emerging capabilities and their broader governance implications.

Future research could extend this analysis through more empirically grounded studies of AI-enabled security operations, particularly in conflict environments. Access to classified, operational, or field-based data could provide deeper insight into real-time decision-making, human–machine interaction, and the operational limits of autonomy in security contexts. Comparative research on AI governance models across different political systems and regions would further enhance understanding of normative competition, regulatory diffusion, and the geopolitical consequences of divergent regulatory approaches.

In addition, sustained attention is required to assess the long-term societal effects of AI-enabled surveillance, automation, and predictive security practices. Questions of public trust, accountability, and democratic legitimacy will become increasingly salient as AI systems are embedded in strategic decision-making processes.

Future scholarship must therefore continue to interrogate the relationship between human agency, technological delegation, and responsibility, ensuring that advances in artificial intelligence contribute to security objectives without undermining the legal and ethical foundations of democratic security governance.

8. BIBLIOGRAPHY

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs.

Bendett, S. (2023). Russian military debates AI development and use. *The Azure Forum*.

Bondar, K. (2025). *Ukraine's future vision and current capabilities for waging AI-enabled autonomous warfare*. Center for Strategic & International Studies.

Boulanin, V. (Ed.). (2019). *The impact of artificial intelligence on strategic stability and nuclear risk: Vol. I (Euro-Atlantic perspectives).* Stockholm International Peace Research Institute.

Boulanin, V., & Verbruggen, M. (2017). *Mapping the development of autonomy in weapon systems*. Stockholm International Peace Research Institute.

Boulanin, V., et al. (2020). *Artificial intelligence, strategic stability, and nuclear risk*. Stockholm International Peace Research Institute.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies, 61*(5).

Campaign to Stop Killer Robots. (2018–2025). *Policy briefs and advocacy reports on lethal autonomous weapons systems (LAWS).* Campaign to Stop Killer Robots.

Csernatoni, R. (2021). *The EU's rise as a defense technological power: From strategic autonomy to technological sovereignty*. Carnegie Europe.

Csernatoni, R. (2024). *Governing military AI amid a geopolitical minefield*. Carnegie Europe.

Docherty, B., et al. (2012). *Losing humanity: The case against killer robots*. Human Rights Watch & Harvard Law School International Human Rights Clinic.

ENISA (European Union Agency for Cybersecurity). (2021). *ENISA threat landscape 2021*. ENISA.

ENISA (European Union Agency for Cybersecurity). (2023). *ENISA threat landscape 2023: Emerging trends in AI and cybersecurity*. ENISA.

ENISA (European Union Agency for Cybersecurity). (2025). *ENISA threat landscape 2025 (preliminary findings).* ENISA.

European Commission. (2019). *Ethics guidelines for trustworthy AI*. High-Level Expert Group on Artificial Intelligence.

European Data Protection Board, & European Data Protection Supervisor. (2021). *Joint opinion 5/2021 on the proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* EDPB & EDPS.

European Data Protection Supervisor. (2023, October 24). *Own-initiative opinion on the Artificial Intelligence Act – Final recommendations*. EDPS.

European Defence Agency. (2021). *ARTINDET – Artificial intelligence for automatic detection, recognition, identification and tracking (final report).* EDA.

European Defence Agency. (2024). *AI for defence – Innovation and research activities overview*. EDA.

European External Action Service. (2022). *A strategic compass for security and defence*. EEAS.

European External Action Service. (2024). *International security and lethal autonomous weapons systems*. EEAS.

European Parliament. (2018, September 12). *European Parliament resolution on autonomous weapon systems (2018/2752(RSP)).*

European Parliament. (2021, January 20). *Resolution on artificial intelligence: Questions of interpretation and application of international law in so far as the EU is affected (2020/2013(INI)).*

European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation).* Official Journal of the European Union.

European Union. (2019). *Regulation (EU) 2019/881 (Cybersecurity Act).* Official Journal of the European Union.

European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* Official Journal of the European Union.

European Union Agency for Fundamental Rights. (2020). *Getting the future right – Artificial intelligence and fundamental rights*. Publications Office of the European Union.

European Union Agency for Fundamental Rights. (2023). *Artificial intelligence and big data: Assessing high-risk AI systems*. Publications Office of the European Union.

Europol. (2023). *Facing reality? Law enforcement and the challenge of deepfakes*. Europol Innovation Lab.

Feldstein, S. (2019). *The rise of digital repression: How technology is reshaping power, politics, and resistance*. Oxford University Press.

Fiott, D. (2018). *Strategic autonomy: Towards "European sovereignty" in defence?* (EUISS Brief No. 12). European Union Institute for Security Studies.

Gkougkoudis, G., Pissanidis, D., & Demertzis, K. (2022). Intelligence-led policing and the new technologies adopted by the Hellenic Police. *Digital, 2*(2), 143–163.

Hellenic Data Protection Authority. (2022). *Decision 35/2022 – Clearview AI biometric data processing.*

Homo Digitalis. (2022). *The Hellenic DPA fines Clearview AI with €20 million.*

Horowitz, M. C., & Scharre, P. (2021). *AI and international stability: Risks and confidence-building measures*. Center for a New American Security.

International Committee of the Red Cross. (2021). *ICRC position on autonomous weapon systems*. ICRC.

Johnson, J. (2019). Artificial intelligence & future warfare: Implications for international security. *Defense & Security Analysis, 35*(2).

Kania, E. B. (2017). *Battlefield singularity: Artificial intelligence, military revolution and China's future military power*. Center for a New American Security.

Kapsokoli, E. (2020). EU cybersecurity governance: A work in progress. In K. Bellou & D. Fiott (Eds.), *Views on the progress of the CSDP* (pp. 65–75). Publications Office of the European Union.

Kapsokoli, E. (2023). Cyberterrorism: A new wave of terrorism or not? In *Hybrid threats, cyberterrorism and cyberwarfare* (pp. 259–280). Springer.

Liaropoulos, A. (2021, June). EU digital sovereignty: A regulatory power searching for its strategic autonomy in the digital domain. In *Proceedings of the 20th European Conference on Cyber Warfare and Security (ECCWS)*. Academic Conferences International.

Liaropoulos, A. (2022). Digital authoritarianism 'Made in China': Installing a Digital Dystopia. *National Security and the Future, 23*(1), 124–139.

Liaropoulos, A. (2024). *Military Artificial Intelligence as an Enabler of European Strategic Autonomy*. Geneva Centre for Security Policy.

Manners, I. (2002). Normative power Europe: A contradiction in terms? *JCMS: Journal of Common Market Studies, 40*(2), 235–258.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology, 6*(3), 175–183.

Pauwels, E. (2020). *The new geopolitics of artificial intelligence*. United Nations University Centre for Policy Research.

Roff, H. M., & Moyes, R. (2016). *Meaningful human control, artificial intelligence and autonomous weapons*. Article 36.

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.

Schmitt, M. N., & Thurnher, J. S. (2013). "Out of the loop": Autonomous weapon systems and the law of armed conflict. *Harvard National Security Journal, 4*, 231–279.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560.

Smuha, N. A. (2021). From a "race to AI" to a "race to AI regulation": Regulatory competition for artificial intelligence. *Law, Innovation and Technology, 13*(1), 57–84.

Sparrow, R. (2007). Killer robots. *Journal of Applied Philosophy, 24*(1), 62–77.

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.

United Nations. (2019). *Report of the 2019 session of the Group of Governmental Experts on emerging technologies in the area of lethal autonomous weapons systems* (CCW/GGE.1/2019/3).

United Nations Convention on Certain Conventional Weapons. (2017–2025). *Group of Governmental Experts on lethal autonomous weapons systems: Meeting reports and guiding principles.* United Nations Office at Geneva.

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International, 22*(4), 97–112.