BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Strategic Management of Emerging Technologies in NATO: A Framework for Foresight, Innovation, and Ethical Integration

Assistant Professor, Abdulkadir AKTURAN*
*Faculty of Economics and Administrative Sciences, Piri Reis University/Türkiye
e-mail: aakturan@pirireis.edu.tr
https://orcid.org/0009-0008-9107-0333

Abstract

The fast rise of artificial intelligence (AI), autonomous systems, and quantum technologies is changing the strategic context of national security. This paper examines how NATO countries can utilize new and Emerging Disruptive Technologies (EDTs) to enhance security and resilience across the Alliance. Using a multi-theoretical framework that combines dynamic capability theory, strategic foresight, military innovation, and technology governance, this discussion explores ways NATO could sense, seize upon, and transform itself in response to technological disruption. This article uses an exploratory qualitative design that combines policy and document analysis to examine institutional policy and lived stakeholder experiences related to technology integration and innovation management. The major issues emerging include variations in capacity for strategic foresight across member states that lead to bureaucratic inertia when some hold back others who want to move forward, put more fragmentation on already piecemeal interoperability standards, and add even more barriers because ethical normative differences are treated as if they belong elsewhere but weigh indeed. Defense Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund infrastructure notwithstanding, national procurement laws, security clearance regimes, and ethical misalignments limit their impacts. Responding to this analysis, therefore, requires proposing a strategic management approach under a four-pillar model that includes strategic foresight, organizational agility, capability integration, and ethical governance. A few of the recommendations are the establishment of a NATO-wide Joint Foresight and Technology Assessment Center, together with harmonization of dual-use procurement procedures, as well as the requirement for mandated national AI ethics frameworks in conformity with alliance-wide interoperability goals. These are steps toward making NATO adaptive and innovative under collective security postures while technological change is accelerated.

Keywords:

Strategic Management; Emerging and Disruptive Technologies; Ethical AI in Defense; Defense Innovation Accelerator; NATO; Military Innovation.

Article info
Received: 25 July 2025; Revised: 29 August 2025; Accepted: 10 September 2025; Available online: 6 October 2025

Citation: Akturan, A. 2025. "Strategic Management of Emerging Technologies in NATO: A Framework for Foresight, Innovation, and Ethical Integration." *Bulletin of "Carol I" National Defence University*, 14(3): 221-244. https://doi.org/10.53477/2284-9378-25-45

Introduction

Emerging and disruptive technologies, accelerating the proliferation of artificial intelligence, autonomous systems, and quantum computing, are changing the nature of modern defense alliances at the strategic level. For NATO, therefore, technological disruption becomes a case of critical opportunity mingled with urgent governance challenges. As military capabilities are reshaped, NATO will have to go beyond responding with changes in operational doctrines and relevant procurement mechanisms by instituting measures that would ensure agility, interoperability, and ethical coherence within its institutional setup. DIANA, the NATO Innovation Fund, and indeed even the Artificial Intelligence Strategy are all important tools recently added to its repertoire, but the innovation ecosystem remains fragmented. Variations at the national level in foresight capacities, procurement regimes, and ethical standards hamper allied efforts toward any collective response regarding rapid technological changes. Existing literature on military innovation and defense modernization primarily discusses either national systems or individual technology-related policies when, in fact, it is systemic and governance-level coordination that is missing within a multilateral institution like NATO. The study will therefore offer a strategic management view of how NATO could implement EDTs successfully across all its member nations, based on a multidimensional framework grounded in four interrelated pillars: strategic foresight, organizational agility, capability integration, ethics, and governance. The analysis is based on dynamic capabilities theory to assess institutional responsiveness; military innovation theory for providing a background to adaptation variability; anticipatory governance, and AI ethics frameworks through which normative issues can be problematized.

This paper uses an exploratory qualitative approach, combined with document analysis of NATO and national strategies, supplemented by examples of NATO member countries. These empirical findings are used to inform the development of a framework in guiding strategic responses to technological disruption.

Hence, this study tries to answer the following questions:

- How can NATO strengthen strategic foresight capabilities across member states to proactively adapt to emerging and disruptive technologies?
- What organizational and bureaucratic constraints hinder NATO's agility, and how can they be overcome to enable timely innovation adoption across the Alliance?
- What are the key technical and regulatory obstacles to achieving interoperability in emerging technology integration across NATO member states?
- How can NATO develop a unified ethical governance framework that reconciles diverse national approaches to AI and autonomous weapon systems?

It, therefore, falls within the strategic management and international security literatures that the paper contributes by offering, thus answering these very pertinent questions, some elements of implementable insights toward future-proofing policymakers for technological posture at NATO.

1. Theoretical Framework

This study applies a multi-theoretical lens in reviewing NATO's strategic management over emerging and disruptive technologies. The lens combines dynamic capabilities theory with strategic foresight, military innovation theory, and technology governance and ethics, thus allowing a comprehensive understanding of organizational, strategic, and normative dimensions regarding technological adaptation within the alliance.

1.1. Strategic Foresight

Strategic foresight is defined as the long-term technological development that could be anticipated within an institution and its potential impact evaluated for providing information for strategic decisions. In NATO's case, strategic foresight would assist in recognizing any new dangers or new possibilities arising and shaping technological priorities, determining where to make long-term investments in defense capability (Kupchyn, Dykhanovskyi and Kolotukhin 2020). A foresight-based approach to strategic foresight requires much more than keeping track of trends in technology; it includes scenario building, technology assessment, and strategic dialogue with stakeholders across the entire alliance. It is also significant to note here that NATO's Allied Command Transformation (ACT) does play a central role regarding strategic foresight; it needs coordination with National Foresight Units and different perspectives integrated towards enhancing the accuracy and relevance of future-looking activities (Nelson, et al. 2021). This paper discusses what changes can be made at the NATO level so that it will help strengthen strategic foresight capacity while anticipating newer technological challenges better.

1.2. Organizational Agility and Bureaucratic Constraints

Technological changes are supposed to be met with organizational agility. Bureaucratic processes, procurement systems, and multidimensional variations of national policies across the Alliance that lock timely innovation even when technological changes elsewhere in the world are embraced remain lodged (Herzog and Kunertova 2024; Shafiabady, et al. 2023). As advanced by the dynamic capabilities theory, this requires new strategic management inspired by a continuous process wherein an organization needs to develop abilities sequentially, sensing the opportunity, then seizing it through strategic action, followed by restructuring its internal structure accordingly (Teece 2007; Bitencourt, et al. 2020). For NATO, such necessary abilities are often limited because of fragmented governance and as a result of institutional inertia. According to dynamic capabilities theory, this means identifying opportunities and threats toward innovation and restructuring the organization to maintain a competitive advantage under rapid changes in environments. For NATO, this theory helps analyze how it can adjust to technological shocks by carrying out environmental scanning and strategic investment activities, which are already being initiated through the Innovation Hub, DIANA, and the NATO Innovation Fund (Herzog and Kunertova 2024). These efforts mark what, in dynamic capabilities terms, is known as the ability of an organization to sense, seize, and transform dimensions of dynamic capabilities. Realizing such potential also requires parallel efforts in breaking bureaucratic barriers and agility enhancement among the member states (Bin 2018).

Institutional theory also considers the role of formal rules in channeling or constraining innovative behavior within large organizations (Scott 2013). Due to NATO's consensus decision-making and the sovereignty of member states, cross-border technological integration is often slowed down. To address such challenges, pathways for increasing flexibility modeled on agile governance, such as experimental procurement frameworks and public-private innovation hubs (e.g., Defense Innovation Unit (DIU), Cyber Innovation Hub (CIH)), could be pathways to further accelerate the adoption of emerging technologies (Rizzo, et al. 2020; Papanikolaou, et al. 2023).

1.3. Technology Integration and Interoperability Challenges

Military innovation theory thus becomes an appropriate approach to explain the uneven technological uptake among NATO member states by considering such key factors as threat perception, leadership orientation, organizational culture, and resource allocation toward new investments and operationalization of technologies (Filip 2022). These differentials within NATO result in different levels of technological readiness that create major problems for interoperability. Other countries whose infrastructure is not adequate and that have a parallel problem with bureaucratic inertia are falling behind the U.S. and U.K., which lead innovation due to strong infrastructure support plus an added dimension of more nimble private sectors involved in defense ecosystems (Horowitz and Pindyck 2022). Apart from widening this structural imbalance, which forms a barrier to overall technology integration, it further slows down the move toward standardization at the alliance level. Military innovation theory can help tease out ways in which these barriers could be lessened by working out how best to get more convergence and coordination across national systems that would drive interoperability for emerging technologies inside alliances.

1.4. Technology Governance and Ethics

Technology governance and ethics relate to normative management issues of dual-use and autonomous systems within disparate jurisdictions. It involves setting ethical considerations regarding the design and application of AI in warfare, ensuring accountability in applying autonomous weaponry, plus the risks correlated with new technological breakthroughs (Wyatt 2023). For NATO, technology governance and ethics acquire a special accent against the background of diversified legal and cultural standards among member states because this is the very ground on which potential ethical disputes can destroy alliance cohesion (Roberson, et al. 2022). NATO faces the daunting task of creating shared ethical principles and governance frameworks that would respect national sovereignty on one hand, but ensure responsible innovation with new technology deployment, on the other (Danks and Trusilo 2022). This study explores how NATO can advance ethical technology governance as well as establish more general consent relating to matters of ethics in emerging technologies.

2. Methodology

This study utilizes a qualitative, document-based research design in probing the strategic management of emerging and disruptive technologies by NATO member states. The qualitative approach of this paper is justified since it endeavors to dwell much on the policy frameworks, institutional mechanisms, and normative dimensions that characterize such complexity in defense innovation and governance on an alliance-wide scale.

2.1. Document and Policy Analysis

The main sources of primary data for this research will be strategic documents, policy papers, and official statements publicly available from NATO and particular member states such as the United States, the United Kingdom, Germany, France, Poland, and Türkiye. Among others, key documents comprise:

- Emerging and Disruptive Technologies Roadmap for NATO.
- NATO Artificial Intelligence Strategy.
- National strategies on AI and defense innovation from the US, UK, and Germany.
- EU Strategic Compass plus appropriate publications of the NATO Innovation Fund.

The review of these documents was done in a systematic manner to extract themes, strategic priorities, and institutional challenges that have increasingly welcomed the adoption of emerging technologies and governance thereof. The selected documents were analyzed using thematic content analysis to extract key themes and insights relevant to NATO's technology strategy and governance. Themes were developed based on key areas of inquiry as established in the literature: strategic foresight, organizational agility, capability integration, and ethical governance. The analysis was manual but informed by a comparative reading across policy frameworks. The coding process was not software-assisted but rather interpretive, with iterative development of categories. It does not quantify frequency but seeks to draw meaningful insights regarding the institutional logic and strategic direction of NATO's technology management. This helps build a conceptual framework based on real-world policy discourse, ensuring academic inquiry as well as relevance to actual policy practice.

3. Findings and Analysis

This section presents an analysis of the findings from the policy and document analysis and expert interviews, focusing on key themes related to strategic management of emerging technologies, ethical considerations, and interoperability challenges within NATO.

3.1. Strategic Foresight across NATO States

Foresight is a strategic capability in leading the anticipation and preparation of possible technological upheavals and emergent threats (Durst, et al. 2014). An adequate level of foresight will enable the Alliance to surface potential opportunities and challenges it may face, inform its strategic decision process, and undertake pre-emptive resource allocation. However, disparities in capacity, coordination, and institutionalization characterize the current landscape of strategic foresight across NATO member states. Such imbalances impede the NATO effort from forming a cohesive, forward-looking approach to innovation in technology and uptake (Martins and Mawdsley 2021). Cyberspace became a crucial national security dimension recognized by NATO as a domain for collective defense, thus requiring military capability development (Bigelow 2019). Processes within Information Technology increase the precision of forecasts relating to any form of threat as well as mitigation so that weapons can be used against targets effectively under contemporary warfare scenarios (Naseem, et al. 2017). The use of Artificial Intelligence in the military has been growing recently and can influence both strategic and operational decision-making levels (Gaire 2023). Firms must invest in training in technical and soft skills to enable employees to maneuver successfully in the continuously changing landscape.

The greater interdependence of systems and reliance on data also enhances cyber risk; hence, robust measures and threat detection techniques should be instituted. Firms should adopt a proactive and future-oriented incident prevention approach, risk management approach, and real-time monitoring. Innovation requires psychologically safe workplaces, whereby employees feel free to share their thoughts with others- such a plan will ensure firms can shift when roles change as AI diffuses by providing learning opportunities for skill development. A cooperative grand cybersecurity strategy is thus required that enables an efficient political-military setup, besides a legal framework within which operational deliverables can take place (Efthymiopoulos 2019). Cooperation with NATO member states helps in resource sharing and specialized know-how through mutual defense arrangements (Reddy 2025). Modernization of European air forces improves defense capabilities for NATO with greater potential as more fifth-generation aircraft are added, decreasing the operational effectiveness of potential adversaries. Firms may also consider taking advantage of new opportunities to integrate cyber threat detection technologies, including AI threat detection and blockchain security technologies, which may assist in understanding evolving and generated cyber threats.

3.1.1. NATO's ACT Innovation Hub and Scenario Planning

The Allied Command Transformation Innovation Hub in Norfolk, Virginia, has been central to the support of long-range scenario planning for NATO (The Innovation Branch of NATO). The Innovation Hub conducts horizon scanning, technology assessments, and wargaming exercises as components in the sensitivity analysis concerning trend input and security environment disruptions. All these activities assist in building strategic insight capacity for long-term plans that NATO has to develop (Efthymiopoulos 2019). However valuable, this results in another problem for the ACT Innovation Hub: There is no coherent work with all national foresight units of NATO member states. This may allow parallel efforts to sprout in other places without drawing on the appropriate synergy and without a concerted approach to strategic foresight within the alliance. Strengthened by regular information sharing, joint workshops, and collaborative research projects, improved coordination mechanisms can make for heightened effectiveness and impact of NATO's foresight activities (Hanna, et al. 2017). NATO is dedicated to enhancing the readiness of its forces to address both present and future defense requirements, modernizing capabilities to safeguard all allies from any threat at any moment, and adopting a more comprehensive and synchronized approach to resilience (Mackenzie 2025). Consistent monitoring, security evaluations, and routine updates to security protocols are essential to sustain the operational resilience of the security framework and mitigate potential risks.

3.1.2. Variations in National Foresight Capacities

Major differences exist in the forecasting capacities of NATO member states. The U.K. and the U.S. Institutionalized forecasting capacity is quite established, with government agencies, research centers, and academic institutions specifically focused on strategic foresight and continuous technology assessment (Slapakova, et al. 2024). These are countries where horizon scanning, trend analysis, and scenario planning investments are made to inform defense and security policies. Some of the smaller NATO allies utilize such capabilities through outside vendors or the ACT Innovation Hub of NATO for strategic foresight activities. Such countries may not have resources, expertise, or even the institutional setup required to build such independent capability in forecasts (Németh, et al. 2018). This puts them in a situation where others external to their state carry out most of the functions and hence cannot root these functions into their specific national context and priorities. Differences in readiness and resilience presuppose variation in foresight capacities among all NATO member states. Some allies have an advantage in readiness to anticipate new threats and opportunities, while others lag behind (Németh, Dew and Augier 2018). Disparities such as these in the collective capacity of the alliance hinder it from responding effectively against multilayered security challenges. As an initial response to such a challenge, NATO may consider initiating capacity-building programs aimed at raising national foresight capabilities among less-resourced member countries (Pataki 2019). Such training could be technical assistance involving the actual funding of these countries in setting up foresight units as well as strategies customized for technology assessment and long-term planning (Nelson, et al. 2021). Furthermore, fostering collaboration and knowledge sharing among NATO members can help bridge the foresight gap, ensuring that all allies benefit from emerging technologies and innovative approaches to security (Pataki 2019). Organizations would benefit from pursuing new opportunities to adopt cyber threat detection technologies, such as AI threat detection and blockchain security technologies, which may be of value for understanding evolving and generated cyber threats.

3.2. Organizational Agility and Bureaucratic Constraints

Organizational agility is the capacity to make adjustments in response to changes in situations, and for NATO to retain its technological advantage amidst technological disruption, it requires high organizational agility (Shafiabady, et al. 2023). Bureaucratic restraints and inflexible structures of organizations hold back an alliance from exercising its full potential in innovation and the right way of integrating new technologies, though (Herzog and Kunertova 2024).

3.2.1. DIANA Initiative and Cross-Border Innovation

One of the great steps towards agile cross-border innovation inside the alliance is the Defense Innovation Accelerator for the North Atlantic initiative (MITRE, 2024). DIANA will bind together innovative startups and technology companies with defense users throughout NATO member countries, offering important funding resources, expertise, and testing facilities (Mahnken 2018). It is this knowledge that DIANA seeks to bring to realization through accelerating cutting-edge technologies that can be applied to defense applications. Collaboration in developing advanced technologies does not guarantee success because of bureaucratic obstacles and regulatory hurdles that DIANA has to work its way around (Wilkinson and Jewell 2017).

The Defense Innovation Accelerator for the North Atlantic (DIANA) was launched in June 2023 as a flagship NATO project to provide support for dual-use technology innovation across the Alliance. It is headquartered in London with regional offices in Tallinn (Estonia) and Halifax (Canada), (Willows 2025). DIANA has 23 accelerator sites and 182 test centers throughout NATO member countries, supported by a value awareness with the NATO Innovation Fund (Collins 2024). DIANA assists startup and research teams exploring emergent technologies in fields such as quantum sensing, AI, autonomy, cyber resilience, and energy. Selected ventures go through a two-phase accelerator process. In the first phase, ventures can receive up to €100,000, and then up to €300,000 for phase two (Vincent 2024). Each phase also includes expert mentorship, access to NATO testing facilities, and opportunities to connect to investors. DIANA's activities align with the NATO Innovation Fund, which aids the development of strategic technologies.

Despite ambitious aspirations, DIANA faces institutional and regulatory challenges. Varied national procurement regulations almost invariably favor domestic providers and inhibit cross-border participation, particularly for start-ups and SMEs. Moreover, differing security clearance processes across NATO members may limit timely access to test facilities and sensitive materials. These challenges hold back the mobility of talent and slow down the adoption of new technology. Nevertheless, DIANA has introduced practices that increase multinational cooperation and flexibility for procurement-like framework agreements and the Rapid Adoption Service. Therefore, DIANA is looking to establish an ecosystem for innovation that is structured and transparent to address legacy defense-industrial fragmentation and make NATO the leader in strategically significant technological innovation (National Defense Magazine 2025; DIANA RFP 2024). National procurement legislations tend to favor programs for newly established yet intently internalized defense contractors and restrict female participation as well as SMEs from other NATO nations (Ablazov and Radov 2020).

3.2.2. Public-Private Innovation Models

NATO may implement public-private innovation models that member states have already initiated. The CIH of Germany and the U.S. Defense Innovation Unit, for example, among others (Rizzo, et al. 2020), were meant to be initiatives through a partnership approach between government, industry, and academia towards development cooperation. Such organizations utilize flexible contractual arrangements, fast-tracked procurement processes, as well as methodologies based on agility for the swift realization of support systems in new technologies, assisting the deployment of innovative solutions. For instance, the CIH provides a program that gives funding access plus mentorship and market opportunities to cybersecurity startups and SMEs (Papanikolaou, et al. 2023). DIU works with commercial technology companies to develop and test prototype solutions addressing specific defense challenges. The private sector can deliver innovation acceleration capabilities that can significantly reduce time lags for capability realization. NATO needs to create collaborative ecosystems with the academic sector and the private sector for a wider reach of resources to build collaborative innovation. Collaborative ecosystems provide organizations with the opportunity to detect new combinations of innovation and leverage market opportunities while reducing risk (Schiuma and Carlucci 2018).

Recommendations

To enhance organizational agility and overcome bureaucratic constraints, NATO should consider the following recommendations:

Harmonize procurement laws and security clearance procedures: Member states should work to harmonize in tandem with NATO procurement regulations and security clearance processes. Barriers to cross-border innovation are reduced when harmonizing such regulations; therefore, more innovative startups and SMEs can participate.

Expand the use of flexible contracting mechanisms: NATO needs to use Other Transaction Authority agreements and more flexible contracting mechanisms, making the procurement process easier and allowing prototyping and experimentation to take place at the speed of relevance.

Foster a culture of experimentation and risk-taking: NATO should foster a culture of experimentation and risk-taking, encouraging defense organizations to embrace new technologies and innovative approaches to problem-solving.

These recommendations will build organizational agility in adopting technological advancements as well as speed up NATO's time to get involved with new technologies, and this will ensure that the alliance stays leading at innovation within the area of defense and security.

3.3. Technology Integration and Interoperability Challenges

A perennial challenge for NATO has been that of technology integration and interoperability due to sundry national systems, sundry levels of technological capacity, and sundry legal and ethical standards. Interoperability does not just mean some technical compatibility; it involves the readiness of systems, units, and forces to function harmoniously together in an integrated fashion.

3.3.1. Federated Mission Networking

NATO's Federated Mission Networking (FMN) architecture is the next big thing, or rather a progressive step in enhancing interoperability across member states (Hanna, et al. 2017). The move by FMN is geared towards coming up with a common technical framework for sharing information and collaboration within multinational operations. Providing standard protocols and interfaces, FMN intends to ease data and service exchanges between various national systems. However advanced FMN has made the world, real-time AI-based interoperability has taken a backseat across platforms, as Buřita et al. (2020) note. The integration of AI technologies into these systems will present new challenges in the field of interoperability due to different data formats, communication protocols, and security standards that will not allow them to efficiently exchange information and coordinate activities.

3.3.2. Alignment of Systems with Data and Legal Standards

Another challenge to the integration of technology into NATO is systems alignment with various data and legal standards (Mbah 2024). Different member states might use varying data formats, communication protocols, and security standards when developing their systems; therefore, it becomes very hard to exchange information and coordinate actions efficiently. Delays, mistakes, and vulnerabilities may be created in an uncoordinated multinational operation as a result of this misalignment. Some systems developed in the U.S., like Project Maven, which applies AI for intelligence analysis, may not immediately be compatible with European data protection regulations such as the General Data Protection Regulation (Schuett 2023).

Such mismatches delay the deployment of such systems within a multinational operation and will require expensive adjustments that will also take time to institute. The absence of common legal standards on the use of AI in military operations would rather open large gaps for legal uncertainty that can equally question NATO's actions' legitimacy and impair its effectiveness (Hill 2020).

Recommendations

NATO may want to prioritize increasing the interoperability of governance frameworks for AI and information-sharing systems within NATO itself and between it and non-NATO stakeholders (Kuziemski and Pałka 2019; Hanna, et al. 2017). Interoperability challenges are, therefore, not only matters for technical consideration but extend to ethics as well in view of the growing decisional autonomy of AI systems. Therefore, to help NATO address issues with technology integration and interoperability, it is recommended that NATO:

Establish Common Data Standards and Protocols: NATO would do well to design and urge the adoption of general data standards and communication protocols for AI systems as a way of ensuring that AI systems created by different member states can easily share information and coordinate activities, thus facilitating the flow of information between various national platforms.

Standardized Security Frameworks: NATO should standardize security frameworks and guidelines for AI systems, such that those systems meet the baseline level of security and resilience against any type of cyberattack or even a simple data breach.

Develop Mechanisms for Cross-Border Data Governance: NATO should put in place cross-border data governance mechanisms, making sure AI systems are in compliance with all relevant data protection regulations and standards of ethics (Mikhaylov, Esteve, and Campion 2018). Such mechanisms will enable secure as well as responsible sharing of information across all national borders while respecting individuals' right to privacy and keeping sensitive information secure (Sharma 2024). Standard protocols for secure information sharing, as well as legal frameworks, are also required by NATO that are compatible with the existing data protection regulations within member states; this means issues on data localization, retention, and access must be addressed so that AI systems can function optimally within diverse legal jurisdictions (Matthews 2022).

Promote the Development of Open-Source AI Platforms: NATO ought to be facilitating the advancement, development, and adoption of open-source artificial intelligence, as this will help enhance transparency and understanding of allied cooperation. This transparency would create the basis for ethical interoperability concerning AI systems if they conformed to the ethics we collectively accept and are accountable in the context of governance. This means NATO could solidify its strategic democratic advantage and strengthen political unity across allied military forces (Danks and Trusilo 2022; Stanley-Lockman 2021).

Promote Joint Experimentation and Testing: NATO must encourage shared trial and error of AI systems in multinational setups, spotting and fixing interoperability issues early on. Dealing with these elements will set the stage for more integration and control steps at the AI–nuclear link (Chernavskikh 2024).
By solving these problems and using these tips, NATO can make it easier to add new technologies and ensure everything works well together with its many systems and tools. Also, NATO should bring back efforts for global rules and get ready for plans led by the United Nations to deal with stopped cyber fights (Taddeo and Floridi 2018).

3.4. Ethics and Governance

The ethical and governance dimensions of artificial intelligence and autonomous weapons systems are vital for NATO to consider, with respect to the likely implications for international security, human rights, and the laws of war (Roorda 2015). The discussions of autonomous weapons systems have raised sizeable legal and moral objections with respect to human control and whether there is a possibility of adhering to international law (Roorda 2015). Different views about the ethics of AI in warfare and the absence of regulatory instruments complicate matters for NATO. In my view, NATO needs to emphasize successfully developing ethical frameworks and governance regimes to ensure the responsible use of AI in defense applications that address ethical considerations throughout the life cycle of any technology from development to operational use (Taddeo, et al. 2021).

3.4.1. Divergent Ethical Approaches

Great divergence and difference of opinion are to be found within the NATO member states regarding the ethical frameworks governing Artificial Intelligence in military applications. Many of these perspectives flow from different national legal traditions, strategic priorities, and societal values. This makes for a complex challenge regarding the harmonization of policy across an alliance.

The United States often highlights AI as a means of gaining both strategic and operational advantages, which makes battlefield management better informed while reducing any time lag in decision-making, as well as ensuring the mitigation of risks to the friendly side, resulting in reduced casualties (Hagos and Rawat 2022). As articulated by Wasilow and Thorpe (2019), AI's capability can be leveraged to enhance situational awareness on the battlefield, speed up decision-making processes, and reduce risk to friendly forces, which consequently would reduce casualties during conflict. The practical benefits that artificial intelligence may provide relating to accuracy and swiftness, as well as effectiveness, are discussed, even regarding the necessity for in-situ learning of legal reviews concerning autonomous systems. This could be reflected in an increased appetite for discovery and subsequent usage of highly autonomous systems in precision targeting or complex logistics operations where the human is not directly involved.

Countries such as Germany and the Netherlands prefer a stricter policy, placing at the first plan of implementation strict adherence to international humanitarian law and fundamental human rights (Hill 2020). The core concern of this policy is to ensure that AI systems, particularly lethal ones, operate within existing legal and ethical frameworks and in meaningful human control in relation to all critical functions they undertake. These are the type of countries that lead advocacies for an international ban-or under very strict regulations on Lethal Autonomous Weapon Systems based on accountability principles and avoiding scenarios where machines may be allowed to make life-and-death decisions without proper human oversight. This ethical decision helps open wider societal debates regarding the morality of transferring such a substantial amount of decision-making authority to machines. Different ethical philosophies can influence national policies on the development and use of AI in military applications. This has become perhaps the most significant challenge to efforts at interoperability and a common strategic approach to AI across the Atlantic Alliance.

3.4.2. Absence of Harmonized Ethical and Regulatory Frameworks

The major challenge that NATO faces in the governance aspect of emerging technologies, especially in the case of autonomous weapon systems, is the absence of a universally binding ethical and regulatory framework. Scholars and experts have continuously identified this vacuum and reiterated the immediate necessity for an extensive, comprehensive set of rules to be developed by the entire alliance for ensuring responsibility in creating and using such systems (McFarland and Assaad 2023).

While the NATO Artificial Intelligence Advisory Board is in the process of efforts towards relevant policy guidance, member states have yet to share a common consensus on what level of human control over Autonomous Weapon Systems (AWS) is necessary and in what particular circumstances these systems can be effectuated both legally and ethically (McFarland and Assaad 2023). This highlights debates that are far from being resolved relating to conceptual and practical challenges toward an adequate prescription of "meaningful human control" within a technological environment increasingly dominated by levels of autonomy and intelligence. This has contributed to the development of a normative vacuum, one with the absence of explicit ethical prescriptions on one hand, and legally enforceable standards on the other. Such a vacuum does not inspire confidence in NATO's ability to control unintended consequences, whether those risks are related to escalation and miscalculation or breaches of international humanitarian law. Complicating matters is the fact that there are fundamental differences in ethical approaches between NATO member states. While some, led by the United States, give primacy to the pursuit of strategic and operational advantages, others, notably Germany and the Netherlands, emphasize international legal and humanitarian normative compliance (Hagos and Rawat 2022; Hill 2020; Wasilow and Thorpe 2019).

Only by bridging those normative differences will it be possible to develop some common ethical approach that would be seen as legitimate across the alliance.

Following the argument presented by Stanley-Lockman (2021), this should not be viewed primarily as a theoretical aspiration but rather forms an integral part of building trust and ensuring meaningful, real interoperability and moral credibility in ever-more-automated situations of conflict. It is here, therefore, that national AI ethics strategies need to match up with NATO's current drive for interoperability. Thus, support comes from Taddeo et al. (2021) in their call for harmonized ethical standards across member states to foster much-needed accountability, together with actual operational coherence and legitimacy in the new age of warfare driven by AI.

3.4.3. The Imperative for International Regulation and United Nations Initiatives

Considering the complications and consequences resulting from autonomous weapons, NATO should encourage and even reinstate efforts for international regulation led by the United Nations (Bode and Watts 2023). Another initiative that would require immediate action is preparing the ground for UN-led initiatives in stalled cyber conflicts, as well as ethical considerations of AI use in warfare; this is also essential for global norm and standard setting. The alliance can extend its hand in international dialogue cooperation by encouraging member states to participate actively in all relevant discussions within the UN concerning matters pertaining to autonomous weapons (Taddeo and Floridi 2018). Such collaboration with other nations and international organizations leads toward comprehensive regulation that is universal to cover the use of such technologies.

Recommendations

To address these ethical and governance challenges, NATO should consider the following recommendations (Matthews 2022):

Work on a unified ethical framework for AI in warfare: Shared values and principles are to lead NATO to the development of a unified ethical framework for AI in warfare. The major aspects that it should cover are human control, accountability, and transparency so that AIs can be used responsibly under existing international laws and with due respect to all ethical standards (Żurek, Kwik and Van Engers 2023). This includes rules for developing, deploying, and using AI-enabled weapons systems as well as means for monitoring and enforcing compliance.

Develop explicit legal norms for AWS: NATO ought to develop explicit legal norms for the design and utilization of autonomous arms, ensuring their compliance with war laws as well as ensuring that they do not pose unacceptable risks to civilians. This involves defining in detail what constitutes the scope of permissible uses, limitations on autonomy as well as safeguards against unintended consequences, and also under circumstances of escalation (Davison 2018). Explicit norms should respond to issues relating to target discrimination and proportionality, and the circumstances under which human intervention is required.

Dialogue and Cooperation on the Consideration of Ethical and Legal Issues: NATO should encourage international dialogue and cooperation on the consideration of ethical and legal issues regarding the use of AI in war with other international organizations and stakeholders, towards establishing common norms and standards. In this regard, NATO can also urge its member states to take a more active role in the relevant UN deliberations and negotiations concerning autonomous weapons (Taddeo and Blanchard 2023). By collaborating with other countries and international organizations, NATO will be assisting in the formulation of detailed codes jointly accepted internationally, controlling the employment of those technologies.

Tackling these ethics and governance challenges, as well as implementing these recommendations, will be important in how well NATO can use the advantages of AI and autonomous systems, meanwhile controlling their risks (McFarland and Assaad 2023). This requires an ongoing conversation that builds consensus between member states on ethical principles and clear ethical guidelines and legal standards reflecting shared values and principles, plus mechanisms to monitor compliance with rules and to address any unintended negative impacts resulting from deploying AI-enabled systems (Dodig-Crnković, Holstein and Pelliccione 2021).

4. Proposed Framework: A Strategic Management Approach

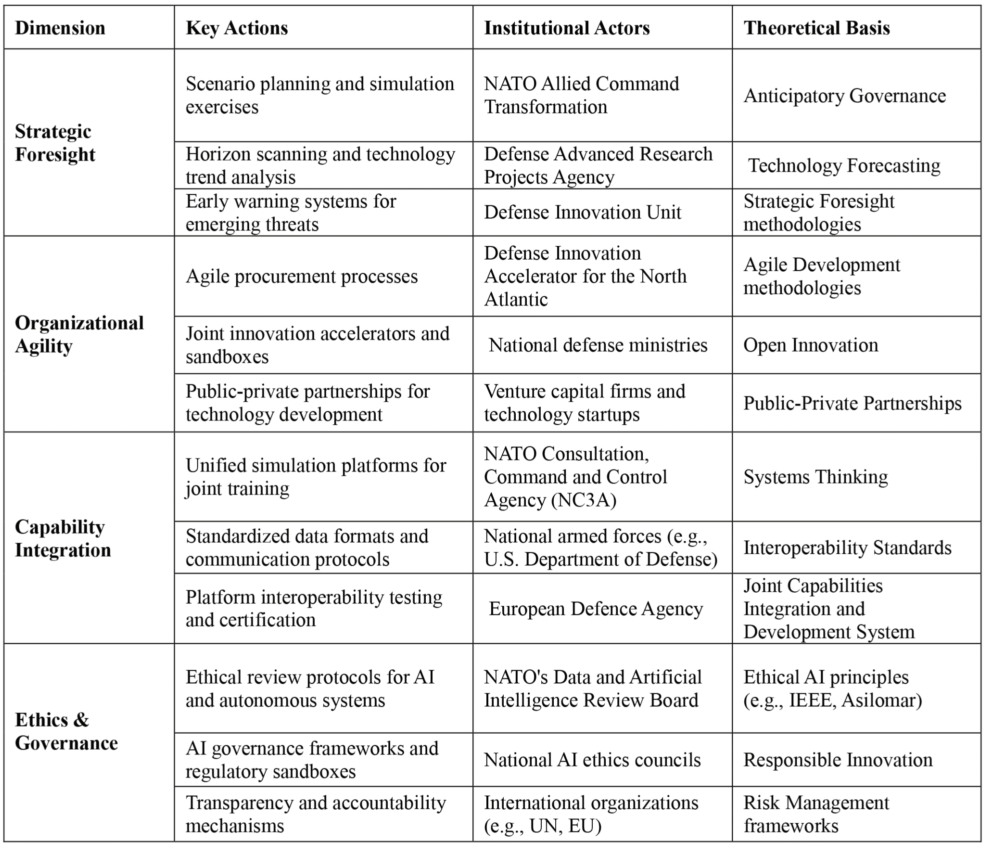
Successful integration and governance of new and emerging technologies in NATO requires a full strategic management framework involving strategic foresight, organizational agility, capability integration, and ethics & governance (Danks and Trusilo 2022). This is, in part, to assist NATO in responding dynamically to the challenges and opportunities offered by new technologies, while remaining true to its traditions, values, and principles (Pataki 2019). By taking a holistic approach to strategic management, NATO can help itself to exploit the opportunities of new technologies to increase its capability, strengthen its partners, and remain competitive in a fast-changing and increasingly complex security environment. Table 1 illustrates this framework:

4.1. Academic Underpinnings

The framework draws from well-known concepts in strategic management, innovation theory, and public policy. Strategic foresight falls within the general principles of anticipatory governance, whose main thrust is an advanced diagnosis of challenges and opportunities that may later be encountered (Khadri 2022). The notion of organizational agility corresponds to the prescription for flexibility and sensitivity in turbulent settings by organizational learning and changing management theory (Shafiabady, et al. 2023). Capability integration borrows from systems thinking and interoperability models, which stress harmonizing different elements

TABLE NO. 1

Strategic Management Framework for Emerging Technologies in NATO Member States



Dimension	Key Actions	Institutional Actors	Theoretical Basis
Strategic Foresight	Scenario planning and simulation exercises	NATO Allied Command Transformation	Anticipatory Governance
	Horizon scanning and technology trend analysis	Defense Advanced Research Projects Agency	Technology Forecasting
	Early warning systems for emerging threats	Defense Innovation Unit	Strategic Foresight methodologies
Organizational Agility	Agile procurement processes	Defense Innovation Accelerator for the North Atlantic	Agile Development methodologies
	Joint innovation accelerators and sandboxes	National defense ministries	Open Innovation
	Public-private partnerships for technology development	Venture capital firms and technology startups	Public-Private Partnerships
Capability Integration	Unified simulation platforms for joint training	NATO Consultation, Command and Control Agency (NC3A)	Systems Thinking
	Standardized data formats and communication protocols	National armed forces (e.g., U.S. Department of Defense)	Interoperability Standards
	Platform interoperability testing and certification	European Defence Agency	Joint Capabilities Integration and Development System
Ethics & Governance	Ethical review protocols for AI and autonomous systems	NATO's Data and Artificial Intelligence Review Board	Ethical AI principles (e.g., IEEE, Asilomar)
	AI governance frameworks and regulatory sandboxes	National AI ethics councils	Responsible Innovation
	Transparency and accountability mechanisms	International organizations (e.g., UN, EU)	Risk Management frameworks

toward the same end (Hill 2020; Porkoláb 2020). The ethics & governance leg sits in ethical canons for creating and using technology, plus modules on responsible innovation and risk management.

5. Discussion: NATO and the Challenge of Technological Disruption

NATO's successful technological engagement with emerging and disruptive technologies underscores the struggle between managing unity at the Alliance level and allowing space for member states' innovation freedom. Even though programs like DIANA and the NATO Innovation Fund were established to centralize and accelerate innovation (Kott, et al. 2018), different strategic prioritizations among member countries and various levels of technological competence across this Alliance continue to decentralize innovation practices (Zhang, Sun and Sun 2023). This situation brings about critical problems in terms of interoperability, standardization, and ethical governance, particularly when talking about artificial intelligence (AI) and autonomous systems' applications (Onderco 2025). The ability of NATO to predict technological disruption will also rely upon a strengthened mechanism in strategic foresight. There is currently no integrated foresight architecture that merges national-level anticipatory planning with the NATO-wide strategy. Though ACT and its Innovation Hub input by way of scenarios and trends, coordination with national foresight units has not been on a consistent basis (Efthymiopoulos 2019). A "Joint Foresight and Technology Assessment Center" could provide comparisons of various national foresight perspectives for synthesis, which in turn would sustain collective strategic planning at the Alliance level to maintain long-term readiness. Where NATO's bureaucracy and different state acquisition processes slow down the timeliness of introducing innovations, organizational agility is equally critical apart from foresight (Herzog and Kunertova 2024). Large states are advantaged by infrastructure and an ecosystem of defense R&D; most small members do not have the human and financial capital to keep up. This creates problems with full participation that work against building momentum collectively (Akhmadi and Tsakalerou 2022; Jurak 2020). Therefore, there is a convincing need for NATO to standardize acquisition rules across its member states and also encourage the formation of joint procurement centers as well as implement experimental procurement forms, including innovation sandboxes and pilot initiatives that can be rapidly tested and afterward scaled up (Maagi and Mwakalobo 2023; Hasik 2024).

Another challenge that brings about other complications in this integration is interoperability. Military innovation theory is central to the explanation of differential rates of technological adoption across the Alliance, with a focus on national variations in threat perception, leadership, and institutional culture (Filip 2022). For example, innovation led by the U.S. and U.K. is followed by others, where bureaucratic inertia, among other shortcomings in infrastructure, happens to be a problem (Horowitz and Pindyck 2022). This creates disparities that later translate into harmonized AI architecture, data-sharing protocols, and cross-border capability integration. To crack these technical and regulatory hindrances, NATO needs advocacy through standardization for public-private investments in collaborative platforms that would forge ways for coordinated development and deployment of dual-use technologies. Perhaps even more formidable would be building common ground concerning an ethical and governance framework relating to AI and autonomous weaponry. The member states are as legally diverse in their ethical concerns related to issues of human control, responsibility, and data rights as the very technology itself complicates joint operations, makes the public lose confidence, and delays efforts at achieving interoperability systems (Aleksandra, et al. 2025; Holst, et al. 2024). In the absence of clearly defined roles and institutional mechanisms for oversight, it is difficult to assign responsibility when an accident takes place (Kandasamy 2024; Pham 2025). NATO should spearhead efforts at harmonization of national AI ethics policies and governance structures that would be transparent in matters relating to accountability as well as compliance with international norms. Cybersecurity has a place in the new order, too. Therein lies the requirements for an integrated cyber strategy encompassing AI-enabled threat detection, infrastructure protection through blockchain on one hand, and adaptive response mechanisms to digital resilience (Bondoc and Malawit 2020; Schiliro 2023; Shiny, et al. 2025). Public-private partnerships and closer collaboration with academic institutions will further support innovation while aligning technical development with strategic needs (Efthymiopoulos 2019; Casady and Garvin 2022). NATO must simultaneously enhance its anticipatory capacities, remove bureaucratic bottlenecks, strengthen interoperability frameworks, and advance a shared ethical vision. Only by addressing these interconnected dimensions can the Alliance maintain its technological edge and strategic coherence in an era defined by rapid and disruptive innovation.

Conclusions

Emerging and disruptive technologies (EDTs) such as artificial intelligence, autonomous systems, and quantum computing grow ever more powerful at a dizzying pace, offering amazing opportunities yet posing daunting dangers for NATO. As proven by this study, managing these strategically within the Alliance calls for a multi-pronged plan that blends foresight with agility, capability integration with ethical governance. Analysis of results brings out into bold relief an urgently critical need for improved bureaucratic capacity at NATO as it tries to pole-vault above barriers in its current rules and regulations against the tide of technological disruption, on the one hand, to encourage interoperability while reconciling widely different ethical and legal standards among member states. The four-pillar framework, consisting of strategic foresight, organizational agility, capability integration, ethics, and governance, gives a holistic approach map through which NATO can find its way around the minefield of technological innovation. A NATO-wide Joint Foresight and Technology Assessment Center, accompanied by harmonized procurement procedures and mandated interoperable ethical frameworks for AI across the Alliance, would go far in bridging this innovation divide and enable collective responses to new forms of threats. Public-private partnerships, on the one hand, will be intensely fostered, and on the other hand, procurement streamlined to finally lead to market-leading technologies being dramatically more rapidly adopted; standardized data protocols and security frameworks themselves create enhanced interoperability.

At the heart of this strategic management approach lies ethical governance. Because ethical views differ between member states, NATO should adopt a consolidated framework that will equally weigh in the balance between providing an operational advantage and observing international humanitarian law as well as human rights laws. NATO has to spearhead the process of creating transparent and accountable as well as legally sound norms for the usage of autonomous systems so that technological advancement is in tandem with the spirit and letter of its founding principles and legal obligations. Ultimately, the achievement of enhanced fusion of EDTs into NATO's strategic posture depends on its adequate dynamism, inclusivity of cooperation, and responsibility in governance. It can do this by heeding the recommendations presented in this paper so as to future-proof its capabilities, reclaim the technological lead, and renew the collective security commitments against a backdrop of fast-paced change that is inherently unpredictable. The road ahead calls for a commitment with equal value to ethical principles, innovation, and multilateral cooperation toward NATO being that resilient, adaptive agent amidst changing global challenges.

References

Akhmadi, S., and M. Tsakalerou. 2022. "Shades of innovation: is there an East-West cultural divide in the European Union?" *International Journal of Innovation Science* 15(2): 260-278. https://doi.org/10.1108/ijis-01-2022-0019

Aleksandra, N., J. Bojana, R. Maryan, and T. Dimitar. 2025. "Evaluating Trustworthiness in AI: Risks, Metrics, and Applications Across Industries." *Electronics* 14(13): 2717. https://doi.org/10.3390/electronics14132717

Bigelow, B. 2019. "What are military cyberspace operations other than war?." In *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1-17). IEEE. https://doi.org/10.23919/cycon.2019.8756835

Bin, A. 2018. "NATO's Defense Institution Building and Projecting Stability." *Connections* 17(3): 8-22. https://doi.org/10.11610/Connections.17.3.01

Binnendijk, A., G. Germanovich, B. McClintock and S. Heintz. 2020. *At the Vanguard: European Contributions to NATO's Future Combat Airpower* (No. RRA3111). https://doi.org/10.7249/rra311-1

Bitencourt, C.C., F. de Oliveira Santini, W.J. Ladeira, A.C. Santos, and E.K. Teixeira. 2020. "The extended dynamic capabilities model: A meta-analysis." *European Management Journal* 38(1): 108-120. https://doi.org/10.1016/j.emj.2019.04.007

Bode, I., and T.F.A. Watts. 2023. Loitering Munitions and Unpredictability. Autonomy in Weapon Systems and Challenges to Human Control. https://findresearcher.sdu.dk/ws/portalfiles/portal/231643063/Loitering_Munitions_Unpredictability_WEB.pdf

Bondoc, C.E., and T.G. Malawit. 2020. "Cybersecurity for higher education institutions: Adopting a regulatory framework." *Global Journal of Engineering and Technology Advances* 2(3): 016-021. https://doi.org/10.30574/gjeta.2020.2.3.0013

Buřita, L., J. Hrabovský, A. Novák, and P. Pohanka. 2020. "Systems Integration in Military Environment." *Advances in Military Technology* 15(1): 25-42. https://doi.org/10.3849/aimt.01334

Casady, C.B., and M.J. Garvin. 2022. "Progressive" Public-Private Partnerships: Are They Reformative or Regressive!?. *Public Works Management & Policy* 27(4): 342-346. https://doi.org/10.1177/1087724x221106164

Chernavskikh, V. 2024. "Nuclear weapons and artificial intelligence: Technological promises and practical realities." *SIPRI Background Paper*. https://doi.org/10.55163/vbqx6088

Collins, E. 2024. *NATO's DIANA Trans-Atlantic Network Expands With New Accelerator, Test Sites.* https://govconexec.com/2024/03/natos-innovation-network-adds-new-accelerator-test-sites/?utm_source=chatgpt.com

Danks, D., and D. Trusilo. 2022. "The challenge of ethical interoperability." *Digital Society* 1(2): 11. https://doi.org/10.1007/s44206-022-00014-2

Davison, N. 2018. "A legal perspective: Autonomous weapon systems under international humanitarian law." In Disarmament (p. 5). United Nations. https://doi.org/10.18356/29a571ba-en

Dewulf, A., and W. Elbers. 2018. "Power in and over cross-sector partnerships: Actor strategies for shaping collective decisions." *Administrative Sciences* 8(3): 43. https://doi.org/10.3390/admsci8030043

DIANA RFP. 2024. *Request for Proposal – Challenge and Accelerator Programme Implementation (NATODX-24-R-0005).* https://www.diana.nato.int/resources/site1/general/rfp%20-%20challenge%20and%20accelerator%20programme%20implementation%20-%20natodx-24-r-0005.pdf

Dodig-Crnkovic, G., T. Holstein, and P. Pelliccione. 2021. " Future intelligent autonomous robots, ethical by design. Learning from autonomous cars ethics." *arXiv preprint arXiv:2107.08122.* https://doi.org/10.48550/arxiv.2107.08122

Durst, C., M. Durst, T. Kolonko, A. Neef, and F. Greif. 2015. "A holistic approach to strategic foresight: A foresight support system for the German Federal Armed Forces." *Technological Forecasting and Social Change* 97: 91-104. https://doi.org/10.1016/j.techfore.2014.01.005

Efthymiopoulos, M.P. 2019. "A cyber-security framework for development, defense and innovation at NATO." *Journal of Innovation and Entrepreneurship* 8(1): 12. https://doi.org/10.1186/s13731-019-0105-z

Filip, S.O. 2022. *Critical success factors for European AI startups.* https://doi.org/10.13140/RG.2.2.19038.72006

Gaire, U.S. 2023. "Application of artificial intelligence in the military: An overview." *Unity Journal* 4(01): 161-174. https://doi.org/10.3126/unityj.v4i01.52237

Hagos, D.H., and D.B. Rawat. 2022. 'Recent advances in artificial intelligence and tactical autonomy: Current status, challenges, and perspectives." *Sensors* 22(24): 9916. https://doi.org/10.3390/s22249916

Hanna, M.W., D. Granzow, B. Bolte, and A. Alvarado. 2017. "NATO Intelligence and Information Sharing: Improving NATO Strategy for Stabilization and Reconstruction Operations." *Connections The Quarterly Journal* 16(4): 5. https://doi.org/10.11610/connections.16.4.01

Hasik, J. 2024. *Friend-sourcing military procurement: Technology acquisition as security cooperation.* https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/friend-sourcing-military-procurement/

Herzog, S., and D. Kunertova. 2024. "NATO and emerging technologies." *Naval War College Review* 77(2): 47-70. https://www.jstor.org/stable/48821934

Hill, S. 2020. "AI's Impact on Multilateral Military Cooperation: Experience from NATO." *AJIL Unbound* 114: 147-151. https://doi.org/10.1017/aju.2020.27

Holst, L., L. Lämmermann, V. Mayer, N. Urbach, and D. Wendt. 2024. *The Impact of the EU AI Act's Transparency Requirements on AI Innovation.* https://aisel.aisnet.org/wi2024/92

Horowitz, M.C., and S. Pindyck. 2022. "What is a military innovation and why it matters." *Journal of Strategic Studies* 46(1): 85. https://doi.org/10.1080/01402390.2022.2038572

Jurak, A.P. 2020. "The importance of high – Tech companies for EU economy – Overview and the EU grand strategies perspective." Research in Social Change 12(3): 32. https://doi.org/10.2478/rsc-2020-0013

Kandasamy, U.C. 2024. *Ethical Leadership in the Age of AI Challenges, Opportunities and Framework for Ethical Leadership.* arXiv (Cornell University). https://doi.org/10.48550/arxiv.2410.18095

Khadri, H.O. 2022. "Becoming future-proof STEM teachers for enhancing sustainable development: A proposed general framework for capacity-building programs in future studies." *Prospects* 52(3): 421-435. https://doi.org/10.1007/s11125-021-09588-0

Kott, A., P. Théron, M. Drašar, E. Dushku, B. LeBlanc, P. Losiewicz, ... and F. De Gaspari. 2018. "Autonomous intelligent cyber-defense agent (AICA) reference architecture. Release 2.0." *arXiv preprint arXiv:1803.10664*. https://doi.org/10.48550/arXiv.1803.10664

Kupchyn, A., V. Dykhanovskyi, and Y. Kolotukhin. 2020. "The war of the future as a strategic guideline for the forming the critical technologies list." *Social Development and Security* 10(1): 9-17. https://doi.org/10.33445/sds.2020.10.1.2

Kuziemski, M., and P. Palka. 2019. *AI governance post-GDPR: lessons learned and the road ahead.* https://doi.org/10.2870/470055

López, O.S. 2025. "Unlocking Regional Economic Growth: How Industry Sector and Mesoeconomic Determinants Influence Small Firm Scaling.“ *Economies* 13(5): 138. https://doi.org/10.3390/economies13050138

Maagi, B., and A. Mwakalobo. 2023. "Practitioners' Perception of the Effect of E-Procurement Practices on Time Saving in Public Procurement in Tanzania." *Open Access Library Journal* 10(5): 1-18. https://doi.org/10.4236/oalib.1110075

Mahnken, T.G. 2018. "Innovation in the interwar years." *SITC Research Briefs* (2018-11). https://escholarship.org/content/qt1hw200dw/qt1hw200dw.pdf?t=p9joni

Martins, B.O., and J. Mawdsley. 2021. "Sociotechnical imaginaries of EU defence: The past and the future in the European defence fund." *JCMS: Journal of common market studies* 59(6): 1458-1474. https://doi.org/10.1111/jcms.13197

Matthews, D. 2022. "UK rejects EU approach to artificial intelligence in favour of 'pro-innovation'policy." *Science Business.* https://sciencebusiness.net/news/uk-rejects-eu-approach-artificial-intelligence-favour-pro-innovation-policy

Mbah, G.O. 2024. "Data privacy in the era of AI: Navigating regulatory landscapes for global businesses." *Int. J. Sci. Res. Anal* 13(2): 2396-2405. https://doi.org/10.30574/ijsra.2024.13.2.2396

Mackenzie, H. 2025. "The North Atlantic Triangle and North Atlantic Treaty: A Canadian Perspective on the ABC Security Conversations of March-April 1948." *London journal of Canadian studies* 38(1): 65-92. https://doi.org/10.14324/111.444.ljcs.2025v38.006

McFarland, T., and Z. Assaad. 2023. "Legal reviews of in situ learning in autonomous weapons." *Ethics and Information Technology* 25(1): 9. https://doi.org/10.1007/s10676-023-09688-9

Mikhaylov, S.J., M. Esteve, and A. Campion. 2018. "Artificial intelligence for the public sector: opportunities and challenges of cross-sector collaboration." *Philosophical transactions of the royal society a: mathematical, physical and engineering sciences* 376 (2128): 20170357. https://doi.org/10.1098/rsta.2017.0357

MITRE. 2024. *Strategic Economics: Options for Competitive Advantage.* https://www.mitre.org/sites/default/files/2024-10/PR-%2024-2927-%20Lessons-Learned-From-NATO-Collaborative-Strategies.pdf

Naseem, A., S.T.H. Shah, S.A. Khan, and A.W. Malik. 2017. "Decision support system for optimum decision making process in threat evaluation and weapon assignment: Current status, challenges and future directions." *Annual reviews in control* 43: 169-187. https://doi.org/10.1016/j.arcontrol.2017.03.003

National Defense Magazine. 2025. *NATO on hunt for innovative defense tech.* https://www.nationaldefensemagazine.org/articles/2025/6/12/nato-on-hunt-for-innovative-defense-tech

Nelson, C., I. Adiguzel, M.V. Florin, F. Lentzos, R. Knutsson, C. Rhodes, ... and A. Vergin. 2021. "Foresight in synthetic biology and biotechnology threats." *Emerging threats of synthetic biology and biotechnology: addressing security and resilience issues*, 177-194. https://doi.org/10.1007/978-94-024-2086-9_12

Németh, B., N. Dew, and M. Augier. 2018. Dew, and M. Augier Understanding some pitfalls in the strategic foresight processes: The case of the Hungarian Ministry of Defense." *Futures* 101: 92-102. https://doi.org/10.1016/j.futures.2018.06.014

Onderco, M. 2025. "Navigating the AI frontier: Insights from the Ukraine conflict for NATO's governance role in military AI." *Journal of Strategic Studies* 48(3): 602-626. https://doi.org/10.1080/01402390.2025.2463451

Papanikolaou, A., A. Alevizopoulos, C. Ilioudis, K. Demertzis, and K. Rantos. 2023. "A Cyber Threat Intelligence Management Platform for Industrial Environments." *arXiv preprint arXiv:2301.03445*. https://doi.org/10.48550/arXiv.2301.03445

Park, S. 2023. "Bridging the global divide in AI regulation: a proposal for a contextual, coherent, and commensurable framework." *Wash. Int'l LJ* 33: 216. https://doi.org/10.48550/arxiv.2303.11196

Pataki, J. 2019. "NATO in 2030 and what the future will bring –'Essential security, dynamic engagement." *Nemzetbiztonsági Szemle* 7(4): 61-70. https://doi.org/10.32561/nsz.2019.4.5

Pham, T. 2025. "Ethical and legal considerations in healthcare AI: innovation and policy for safe and fair use." *Royal Society Open Science* 12(5): 241873. https://doi.org/10.1098/rsos.241873

Porkoláb, I. 2020. "An AI Enabled NATO Strategic Vision for Twenty-First-Century Complex Challenges." In *Artificial Intelligence and Global Security* (pp. 153-165). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78973-811-720201009

Reddy R.P. 2025. "Cyber Warfare: National Security Implications and Strategic Defense Mechanisms." *International Journal of Computer Trends and Technology (IJCTT)* 73*(*4): 48-59. https://doi.org/10.14445/22312803/ijctt-v73i4p107

Rizzo, F., F. Schmittinger, and A. Deserti, A. 2020. "Expanding innovation capacity in public sector by design projects." *Proceedings of DRS* 5: 1993-2009. https://doi.org/10.21606/drs.2020.355

Roberson, T., S. Bornstein, R. Liivoja, S. Ng, J. Scholz, and K. Devitt. 2022. "A method for ethical AI in defence: A case study on developing trustworthy autonomous systems." *Journal of Responsible Technology* 11: 100036. https://doi.org/10.48550/arxiv.2206.10769

Roorda, M. 2015. "NATO's Targeting Process: Ensuring Human Control Over and Lawful Use of 'Autonomous' Weapons." *Mark Roorda, NATO's Targeting Process: Ensuring Human Control Over (and Lawful Use of)'Autonomous' Weapons, in: Autonomous Systems: Issues for Defence Policymakers, eds. Andrew Williams and Paul Scharre, NATO Headquarters Supreme Allied Command Transformation, Amsterdam Center for International Law*, (2015-06). https://ssrn.com/abstract=2593697

Schiliro, F. 2023. "Building a resilient cybersecurity posture: a framework for leveraging prevent, detect and respond functions and law enforcement collaboration." *arXiv preprint arXiv:2303.10874*. https://doi.org/10.48550/arxiv.2303.10874

Schiuma, G., and D. Carlucci. 2018. "Managing strategic partnerships with universities in innovation ecosystems: A research agenda." *Journal of Open Innovation: Technology, Market, and Complexity* 4(3): 25. https://doi.org/10.3390/joitmc4030025

Schuett, J. 2023. "Risk Management in the Artificial Intelligence Act." *European Journal of Risk Regulation* 15(2): 367. https://doi.org/10.1017/err.2023.1

Shafiabady, N., N. Hadjinicolaou, F.U. Din, B. Bhandari, R. Wu, and J. Vakilian. 2023. "Using Artificial Intelligence (AI) to predict organizational agility." *Plos one* 18(5): e0283066. https://doi.org/10.1371/journal.pone.0283066

Sharma, D.N. 2024. "Artificial intelligence: Legal implications and challenges." *Knowledgeable Research A Multidisciplinary Journal* 2(11): 13-32. https://doi.org/10.57067/220k4298

Shiny, J.M. DrK. V., K. Rohith, C.B.R. Reddy and C. Ganesh. 2025. "AI Powered SOCs Detect and Respond to Cyber Security Threats in Real Time by using Deep Learning." *International Journal of Innovative Research in Science engineering and Technology* 14(4). https://philarchive.org/rec/DRKAPS

Slapakova, L., A. Fraser, M. Hughes, M.C. Aquilino, and K. Thue. 2024. *Cultural and technological change in the future information environment*. RAND. https://doi.org/10.7249/rra2662-1

Stanley-Lockman, Z. 2021. "Responsible and ethical military AI." *Centre for Security and Emerging Technology*. https://doi.org/10.51593/20200091

Taddeo, M., and A. Blanchard. 2023. "A comparative analysis of the definitions of autonomous weapons." In *The 2022 yearbook of the digital governance research group* (pp. 57-79). Cham: Springer Nature Switzerland. https://doi.org/10.1007/s11948-022-00392-3

Taddeo, M., and L. Floridi. 2018. "Regulate artificial intelligence to avert cyber arms race." *Nature* 556 (7701): 296-298. https://doi.org/10.1038/d41586-018-04602-6

Taddeo, M., D. McNeish, A. Blanchard, and E. Edgar. 2022. "Ethical principles for artificial intelligence in national defence." In *The 2021 Yearbook of the Digital Ethics Lab* (pp. 261-283). Cham: Springer International Publishing. https://doi.org/10.1007/s13347-021-00482-3

Tomada, L. 2022. "Start-ups and the Proposed EU AI Act: Bridges or Barriers in the Path from Invention to Innovation?." *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 13: 53.

Vincent, B. 2024. *NATO's innovation accelerator begins search for its second cohort.* https://defensescoop.com/2024/07/01/nato-innovation-accelerator-diana-begins-search-second-cohort/?utm_source=chatgpt.com

Wasilow, S., and J.B. Thorpe. 2019. "Artificial intelligence, robotics, ethics, and the military: A Canadian perspective." *Ai Magazine* 40(1): 37-48. https://doi.org/10.1609/aimag.v40i1.2848

Weerasinghe, R.N., and A.K.W. Jayawardane. 2019. "The Art of Crafting Actionable National Innovation Policy: The Case of Sri Lanka." *Journal of Economics and Business* 2(4). https://doi.org/10.31014/aior.1992.02.04.163

Wilkinson, M., and S. Jewell. 2017. "Defence requires Enterprise-Level Innovation: Using a Systems Approach to secure superior Value from Ideas." In *INCOSE International Symposium* 27(1): 87-101). https://doi.org/10.1002/j.2334-5837.2017.00347.x

Willows, M. 2025. *DIANA: NATO's Innovation Powerhouse Springs into Action.* https://ddrc.uk/diana-natos-innovation-powerhouse-springs-into-action/?utm_source=chatgpt.com

Wyatt, A. 2023. "Examining Supply Chain Risks in Autonomous Weapon Systems and Artificial Intelligence." *Applied Cybersecurity & Internet Governance* 2(1): 1-21. https://doi.org/10.60097/acig/162874

Young, T.D. 2019. "NATO's selective sea blindness." *Naval War College Review* 72(3): 12-39. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8041&context=nwc-review

Zhang, G., J. Sun, and Y. Sun. 2023. "Mapping interdisciplinary collaboration in music education: analysis of models in higher education across North America, Europe, Oceania, and Asia." *Frontiers in Psychology* 14: 1284193. https://doi.org/10.3389/fpsyg.2023.1284193

Zurek, T., J. Kwik, and T. Van Engers. 2023. "Model of a military autonomous device following International Humanitarian Law." *Ethics and Information Technology* 25(1): 15. https://doi.org/10.1007/s10676-023-09682-1

ACKNOWLEDGEMENTS

I express my gratitude to Professor Mehmet Ziya SÖĞÜT for his support and guidance.

FUNDING INFORMATION

N/A

CONFLICT OF INTEREST STATEMENT

The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are openly available on the internet.

DECLARATION on AI use (if applicable)

N/A