# AI: THE BEAST THAT FEEDS THE BEAST IN THE PERFECT STORM OF HYBRID WARFARE

**Carola FREY**

PhD Student, The National School of Political Science and Public Administration, Bucharest, Romania

***Abstract:*** *The present paper examines the dual-use nature of AI (its capacity to serve both civilian and military applications) and its role in amplifying hybrid threats. Drawing on a qualitative methodology that includes literature review and strategic foresight methods, the study analyzes how AI technologies are being integrated into conflict environments. A key focus is placed on the role of data as both a foundational asset and a crucial point of vulnerability. AI systems depend on large datasets for training and performance, yet this dependence also exposes them to manipulation, corruption, and adversarial exploitation. As such, control over data is rapidly becoming a central element of strategic competition. The paper presents five future-oriented scenarios to illustrate how dual-use AI can lead to unpredictable escalations, compromised infrastructures, and blurred distinctions between civilian and military domains. These scenarios provide actionable insights into potential developments, including the risks posed by open-source proliferation, AI-enabled disinformation, and compromised supply chains. Ultimately, this study argues for the need to embed ethical principles, regulatory oversight, and anticipatory governance into AI development and deployment. Without robust safeguards and a commitment to resilience, AI may evolve into a destabilizing force in hybrid warfare, accelerating arms races and undermining international stability rather than enhancing security.*

***Keywords****: artificial intelligence; dual-use technologies; hybrid warfare; resilience; strategic foresight*

## 1. INTRODUCTION

Artificial intelligence (AI) has increasingly become a dominant theme across academic, political, media and strategic discourse. Driven in part by a growing fear of being left behind, AI is now prominently featured in major policy reports, international conferences, and public debates. Despite the lack of specific conceptual boundaries, its perceived potential to transform nearly every domain of society (economics, politics, warfare, and daily life) has promoted it to a central position in global discourse (often framed as comparable in scale to electricity or a full industrial revolution). The growing interest reflects not only the tangible capabilities of AI, but also the broader expectations, strategic ambitions, and underlying anxieties that societies associate with emerging technologies. While the enthusiasm surrounding AI can sometimes be speculative or overstated, it is nonetheless grounded in the very real and transformative impact this technology is beginning to exert across both civilian and military domains. For the purposes of this paper, AI is understood as *agents that receive percepts from the environment and perform actio*ns (Russell & Norvig, 2020:31-40), a definition that emphasizes its functional and decision-making capabilities within dynamic environments. Central to AI's functionality are data and algorithms. Data serves as the foundational input, enabling AI systems to learn and make decisions. Algorithms, on the other hand, provide structured procedures that process this data to produce desired outcomes (Hurbans, 2020:3-6).

The objective of this article is to explore the dual-use nature of AI and its implications for contemporary security dynamics, with particular emphasis on hybrid threats and ethical challenges. In line with this objective, the guiding research question is: *How does the dual-use nature of AI contribute to hybrid threats and strategic vulnerabilities?* This research adopts a qualitative approach grounded in literature review, comparative analysis, and scenario-based foresight. The study draws on a broad range of sources, including academic books, peer-reviewed journal articles and policy reports. These materials provide the foundations for understanding the dual-use nature of AI, as well as the operational, ethical, and strategic dimensions of its application.

To assess potential future developments, the study applies foresight methods, specifically trend

analysis and scenario development, to identify emerging risks linked to AI in the military domain, ethical issues and hybrid threats. While this study does not involve new primary data collection, it incorporates original findings from the author's previous research in the field (which includes foresight workshops, expert interviews, and consultations with practitioners). These insights, combined with existing literature, support a forward-looking analysis of emerging trends and risks. One limitation of this approach is its reliance on secondary sources and existing data, which may not fully capture rapidly evolving developments or classified dimensions of military AI use. To address this, the study integrates foresight methods that enable exploration of plausible futures beyond the constraints of currently available data, thereby enhancing its relevance for anticipating and mitigating emerging risks.

## 2. DELINEATING AI'S DUAL-USE POTENTIAL

Hal Brands and Charles Edel (2019) argue that the postwar international order was constructed upon a collective memory of past catastrophes of two world wars and the Cold War and a firm determination to prevent their recurrence. War was envisioned as something to be memorialized rather than re-experienced, serving as a reminder of tragedy rather than a recurring event. Despite these aspirations, the hope that war could be definitively eliminated proved overly optimistic. Rather than disappearing, conflict evolved, adapting itself into novel forms, especially through emerging technological innovations within cyberspace and digital realms. Technological advancements, from aircraft to mechanized vehicles, have consistently reshaped the nature of warfare (Freedman, 2013). Current technological developments continue this trajectory, introducing elements such as data-driven surveillance, cyberattacks, drones, hybrid threats, algorithmic manipulation, and mis- and disinformation campaigns.

Artificial intelligence, promoted constantly as a transformative force, is becoming increasingly central to debates around the nature of future conflicts (Romele, 2024, Payne, 2023). AI has often become a catch-all label encompassing big data, machine learning, automation, and a range of computational advances. This conceptual ambiguity complicates both public understanding and policy development, particularly when assessing the strategic implications of AI in military contexts. This technology fuels both practical innovations and intense speculation, building perceptions of warfare as potentially risk-free, remote, and morally detached. AI-enabled systems promise enhanced speed and precision, but more importantly, they introduce the possibility of shifting ethical and legal responsibility away from humans. Military programmers, operators, and political leaders become progressively distanced from direct accountability as decision-making becomes outsourced to algorithms (Johnson, 2022). This fosters the dangerous illusion of a rational, sanitized form of warfare, presented as capable of transcending human limitations, and simultaneously dehumanizing the battlefield and diluting lines of responsibility.

Integral to these developments are the narratives and imaginaries constructed around AI. These stories range from realistic portrayals grounded in technological realities to speculative and culturally influenced visions shaped by fear, desire, or aspiration (Cave & Dihal, 2023; Cave *et al.*, 2020). Such narratives not only reflect what AI is currently capable of, but project collective expectations: an extension of human control, a potential savior, a threatening rival, or a substitute for human judgment. Within military contexts, these imaginaries significantly influence strategic thinking and operational expectations, sometimes presenting AI as a nearly autonomous actor. In doing so, they obscure the reality that AI systems remain, at their core, algorithmic tools trained on datasets vulnerable to human biases, operational constraints, strategic framing, and deliberate adversarial manipulation.

Moreover, as highlighted by Galdorisi and Tangredi (2024), AI technology is no longer exclusive to major powers or futuristic scenarios. The dual-use character of AI, coupled with its widespread open-source accessibility, accelerates its adoption by diverse actors seeking geopolitical advantage (Pandya, 2019). AI is already employed in mis- and disinformation campaigns aimed at destabilizing democracies, and its integration with commercially available drones produces cost-effective autonomous weapons. Guilong Yan (2020) further emphasizes AI's transformative role in reshaping the character of hybrid warfare by intensifying its inherent features - synergy, ambiguity, asymmetry, disruption, and psychological manipulation. AI enables hostile actors to operate simultaneously across military, political, economic, civil, and informational domains. Consequently, distinctions between war and peace, civilian and combatant, truth and deception become increasingly blurred. AI-

powered tools amplify the scope, velocity, and impact of adversarial actions, creating profound and persistent challenges.

The concept of dual-use technologies can be interpreted through multiple lenses; however, for the purposes of this article, the analysis will focus on two specific frameworks, excluding, for instance, interpretations of dual-use as good vs. bad. First, it refers to technologies that can serve both military and civilian (non-military) purposes (Miller, 2018:14; Vaynman & Volpe, 2023). Second, it includes technologies initially developed for civilian use but easily repurposed or modified for military applications. This second framework is particularly relevant because the reverse process, adapting military technologies for civilian use, is often more complex and limited. Military systems are typically designed for specific operational contexts, involve classified components, and are governed by strict security protocols. These factors can make their transition to civilian markets impractical, costly, or legally restricted. However, these definitions are not mutually exclusive; in practice, many technologies meet both criteria, reflecting the thin boundaries between civilian and defense innovation. To further clarify this dual-use nature, Vaynman and Volpe (2023) introduce two key analytical dimensions: distinguishability and integration. Distinguishability refers to how easily one can differentiate a technology's civilian and military applications. While some systems, like battleships, are clearly distinct from commercial cargo vessels, others, such as drones, often appear and function similarly in both contexts. Integration, on the other hand, concerns how extensive technology is present in both the civilian dynamics and military operations. Some technologies, like long-range rockets, are used narrowly for strategic or space-related missions. Others are widely used in both commercial and military domains, increasing the complexity and risk associated with inspections or regulatory oversight (Vaynman &Volpe, 2023). Applied to AI, this framework reveals that AI has low distinguishability, as many systems (such as image recognition, language processing, or autonomous navigation) can be used in both civilian and military contexts with minimal modification. Its high integration means that AI is not confined to specialized defense systems but is widely embedded in both military infrastructure and civilian sectors (ranging from healthcare and finance to logistics and communications). This situation makes regulatory oversight complex, as any restriction on military AI use may inadvertently affect essential civilian applications. Furthermore, the situation becomes even more complex when AI systems are developed by private companies. Although primarily intended for commercial use, these systems often possess architecture and capabilities that can be readily adapted for military purposes (Galdorisi & Tangredi, 2024:11). One major point of contention involves exactly the role of private companies developing AI technologies. While some AI systems, such as those trained on openly available satellite datasets for geospatial intelligence analysis can be adapted for military use, others are limited by the nature of the data they are trained on. Commercial datasets may be suitable for civilian applications but often lack the specificity, sensitivity, and strategic relevance required for defense contexts. Military-grade AI systems demand access to classified or highly specialized datasets that governments are typically unwilling to share, especially with private actors or across national borders. And nevertheless, even when such data is available, it remains inherently past-oriented (Borchert *et al.*, 2024:5-6). Thus, it creates a barrier in translating commercially developed AI into effective military tools, and the involvement of private actors also raises issues of control, accountability, and access to sensitive capabilities beyond state oversight.

In addition, the dual-use nature of AI can go easily beyond the original intentions of their developers and can potentially be corrupted. AI technology can fail when repurposed for military applications if not properly conceptualized and implemented. If originally intended for civilian use, such technology adheres to specific rules and is trained on data aligned with non-military needs. When it is adapted for military purposes, the underlying civilian-oriented data used for training may prove inadequate, leading to operational and drastic failures (Borchert *et al*, 2024). In these cases, the failure of the technology is not only a result of its unsuitability for military use, but also a consequence of the original developers' failure to anticipate and address these dual-use challenges. As a result, technology is misapplied in ways that undermine its original purpose and effectiveness.

Moreover, a particularly problematic scenario arises when a state, lacking the resources or capacity to develop its own technology, relies on external, proxy, or third-party sources to acquire it. Such a source, either a foreign company or a government, may then repurpose the technology that was for military use or manipulate its civilian application to advance its strategic objectives. This situation poses a significant risk because

technology can be used in ways that go beyond the original intent of the user, turning it into a Trojan horse. If the technology acquired is intended for military purposes from the outset, the stakes are even higher, as it becomes a national security issue and a significant risk (and there is no guarantee how or when it will be used to benefit those who control it, making it potentially a high-stakes gamble). Another critical risk emerges when dual-use technology is compromised by external actors who modify or hack it without the knowledge or consent of the original developers or current users, posing a significant security risk. AI, with its opaque algorithms and specialized training data, is an excellent example. Malicious actors could infiltrate the system, manipulate its functions, or deliberately cause it to fail. This represents a distortion of technology's intended purpose, leading to potential misuse and significant vulnerabilities. In any context, AI systems could be corrupted if the data they are trained on is flawed (biased) or intentionally poisoned by adversaries. Additionally, AI systems can be exploited by targeting vulnerabilities in their "thinking" processes, like cognitive hacks that resemble cyberattacks on computer software (Scharre, 2023).

These examples illustrate that the dual-use character of artificial intelligence entails not only operational and regulatory complexities, but also ethical and strategic implications. While the potential benefits of AI, when properly designed, implemented, and governed, are clear and widely acknowledged, this ideal is not always reflected in practice. In many cases, AI technologies are deployed without sufficient oversight, ethical safeguards, or contextual alignment, often driven by the desire to secure a first-mover advantage (Johnson, 2023:12), which can lead to unintended consequences and systemic vulnerabilities.

## 3. PRELIMINARY FINDINGS OF TOPIC-RELEVANT TREND ANALYSIS

Over the next decade, and even within the next five years, AI's role is expected to expand significantly among major powers. Key trends driving this expansion include the development of autonomous weapons systems and swarm technologies. They are increasingly designed to operate with minimal human intervention, enhancing their speed, mobility, and operational flexibility (Fox, 2024). Notably, this includes systems capable of autonomously selecting and engaging targets without direct human oversight, as well as those designed to coordinate attacks in a distributed, self-organizing manner. Such an example can be seen highlighted in a UN report on the conflict in Libya, where autonomous drones were used to hunt down retreating fighters, reportedly operating without requiring data connectivity between the operator and the munition. This effectively demonstrated a "fire, forget, and find" capability, in which the system could independently locate and engage targets after launch (United Nations Security Council, 2021:17). The deployment of such unmanned combat aerial vehicles, along with smaller drones used for intelligence, surveillance, and reconnaissance, exemplifies the growing autonomy of military systems and the erosion of direct human control in life-and-death decisions. These developments put pressure on the need for human oversight, accountability and international humanitarian law.

Another key trend is the integration of AI-enabled intelligence and decision-support systems, which militaries are increasingly employing to process vast amounts of data for surveillance, reconnaissance, and targeting (Simpson et al. 2025). These systems excel at pattern recognition across images, signals, and even social media, enhancing threat detection capabilities. Commanders are beginning to rely on AI tools for wargaming scenarios and operational planning (Ong, 2021). Within the next five years, such decision-support systems may become routine, potentially accelerating the pace of warfare, though not without risks of error. Looking ahead, AI could be embedded into command-and-control networks, enabling real-time coordination across land, air, sea, cyber, and space domains with unprecedented speed and integration.

Another major emerging trend is the growing role of AI in enabling information warfare and intensifying hybrid threats. AI is rapidly becoming a core component of hybrid operations, particularly through its use in generating and amplifying deceptive content. Tools such as deepfakes, generative media, and synthetic audio and video can fabricate highly believable narratives, simulate credible individuals, and manufacture the illusion of public consensus (Mazzucchi, 2022). Beyond spreading mis/ disinformation, these technologies can construct persuasive but false statements, manipulate perception, and erode trust in information ecosystems, all with minimal human intervention.

AI is becoming a powerful tool in the cyber domain, capable of identifying vulnerabilities,

automating attacks, and adapting offensive operations in real time. Offensive AI-based cyber instruments are becoming increasingly widespread, highlighting their dual-use nature as they can be developed for legitimate cybersecurity purposes but easily repurposed. This dual-use potential significantly amplifies the risks in hybrid conflict scenarios, as both state and non-state actors can exploit these tools to disrupt systems and manipulate digital environments.

Furthermore, the "democratization" of AI represents a significant shift from historical patterns of technological development, where innovation was largely driven and controlled by military institutions (Black *et al.*, 2024:3). Today, advances in AI are primarily led by the commercial sector, making the technology widely accessible and rapidly diffused across the globe. As a result, AI is no longer the exclusive domain of superpowers; even smaller states and non-state actors can access and deploy advanced AI tools.

These trends highlight also urgent ethical and regulatory challenges. While institutions like the EU Parliament advocate banning fully autonomous lethal systems, strategic competition continues to drive development. Regulatory efforts lag behind, in part because AI is intangible, dual-use, and difficult to classify. No binding global treaty exists, and recent initiatives, such as the U.S. political declaration and the Dutch summit on responsible military AI (2023), signal progress, but global consensus remains elusive.

Accountability is another concern, as opaque algorithms complicate legal responsibility in cases of civilian harm (Csernatoni, 2024). Ensuring AI compliance with international humanitarian law is both a technical and ethical challenge, especially given potential bias in training data. While Western militaries are adopting ethical principles, enforcement is inconsistent.

AI can provide faster decision-making and enhanced capabilities, but it introduces risks. Technically, AI systems are prone to errors such as target misidentification, adversarial manipulation, data poisoning, and supply chain vulnerabilities, raising serious concerns about reliability in combat scenarios. Operationally, autonomous systems can behave unpredictably, and their opaque decision-making may lead to either overreliance or mistrust. Risks like automation bias and accelerated conflict tempo pose challenges for command structures and human oversight. Strategically, it accelerates the arms race dynamics, erodes deterrence stability, and increases the risk of proliferation to rogue actors or non-state groups. Without robust governance, human control, resilience frameworks and confidence-building measures, military AI could become a major driver of global instability.

Beyond dominant trends, several weak signals can be identified, like AI-augmented wargaming and strategic planning (with early experiments showing promise in simulating adversary behavior and generating novel tactics). Non-state actors, including militias and criminal networks, have begun experimenting with AI tools like deepfakes and autonomous drones. While isolated now, their growing access to open-source AI could pose new threats.

Several low-probability but high-impact wild cards can also be examined. One possibility is accidental escalation, where an AI defense or early-warning system misinterprets an event (for example as a hostile act) triggering unintended military conflict. Such an incident could provoke international backlash. Another wild card is a breakthrough toward advanced AI or Artificial General Intelligence. A sudden leap in capabilities could grant a single actor overwhelming strategic advantage, destabilizing global power balances and igniting an arms race (or conversely, forcing cooperation through deterrence).

A third situation involves a non-state actor acquiring AI super-weapons. Though currently unlikely due to technical barriers, such a case becomes more plausible if the actor acquires commercially available, civilian AI systems and repurposes them using internal expertise and resources. Such a case would allow for the development of powerful tools that rival state capabilities.

## 4. FIVE POSSIBLE RISK SCENARIOS

To explore the evolving security implications of AI's dual-use nature, this section employs as a methods scenario building to examine several potential futures. Drawing on the trend analysis, these following scenarios illustrate how AI can amplify hybrid threats, expose strategic vulnerabilities, and challenge existing regulatory frameworks. While speculative in nature, each scenario is grounded in observable developments and serves to anticipate potential risks, stress-test assumptions, and inform future policy.

The first scenario proposes a commercial AI-based facial recognition system, originally developed for smart city infrastructure, is repurposed by a state actor for surveillance in contested territories. The technology, embedded in civilian CCTV networks, is linked to a centralized

military command structure that uses it to identify and detain political dissidents and perceived insurgents. The system's civilian origins obscure its militarized application, evading international scrutiny. This scenario underlines the challenge of low distinguishability in dual-use AI, as well as the risks of civilian infrastructure being militarized covertly. It points out how dual-use AI can facilitate hybrid authoritarian strategies that blend domestic control with strategic denial. It also raises concerns about accountability and verification mechanisms in export control regimes.

The second scenario takes place during a regional border standoff, where an autonomous loitering munition misidentifies a surveillance drone as a hostile asset and engages it without human oversight. The incident triggers a retaliatory cyberattack from the opposing state. Due to algorithmic opacity and communication delays, human commanders are unable to confirm the chain of events before escalation occurs. What this scenario points to is the strategic risk of automated decision-making in crisis situations, particularly where human oversight is disregarded. It underscores the necessity for meaningful human control, and the development of autonomous engagement norms to prevent unintentional conflict escalation. It also reveals the tempo mismatch between AI systems and diplomatic channels in high-stakes settings.

Third, in the scenario a mid-level power contracts a private foreign vendor to develop an AI-enabled logistics system for national critical infrastructure. The vendor includes hidden surveillance functions in the software, allowing a rival state to map and eventually disrupt key military supply routes during a regional conflict. The embedded system is activated remotely during a hybrid campaign. In this case, it can be demonstrated the vulnerability of AI supply chains, especially where foreign-developed systems are integrated into dual-use national infrastructure. It highlights the need for technological due diligence, source auditing, and the creation of AI integrity verification mechanisms to prevent adversarial manipulation of embedded civilian technologies.

The fourth scenario can take the form of a non-state actor that adapts open-source AI navigation code, originally designed for agricultural drones, into a low-cost swarm system targeting energy infrastructure. The attack demonstrates unexpected effectiveness, inspiring similar efforts by other groups. The proliferation of easily accessible dual-use AI destabilizes deterrence dynamics and overwhelms conventional defense mechanisms. From this scenario is underlined the democratization of AI-based warfare through open-source tools, challenging traditional state monopolies on high-end technologies. It emphasizes the risks of unregulated dual-use code dissemination and necessitates the development of norms for open-source AI governance to mitigate proliferation risks.

In the fifth scenario, and the last, an AI-enabled port management system, implemented to optimize maritime logistics, is compromised via software vulnerability inserted by a foreign subcontractor. During a geopolitical crisis, this vulnerability is activated: cargo ships are misclassified, coast guard vessels are deprioritized, and false manifests enable the insertion of surveillance devices into critical maritime infrastructure. This scenario underscores the hybrid risks of AI integration in maritime infrastructure, particularly where civilian logistics systems intersect with naval operations. It raises concerns over infrastructure sabotage, supply chain infiltration, and the blurring of civil-military boundaries. It also highlights the urgent need for AI security protocols in smart port systems and civil-military resilience planning in the maritime domain.

## 5. CONCLUSIONS

This study has looked in the dual-use nature of artificial intelligence and its implications for contemporary dynamics, with particular attention to the risks posed by hybrid threats, data vulnerabilities, and civil–military convergence. Through an integrated approach that combined literature review, trend analysis and scenario development, the research has shown that AI, while offering enhanced operational capabilities, simultaneously generates complex ethical dilemmas and strategic vulnerabilities. The scenarios presented illustrate how AI can be repurposed, manipulated, or misused in ways that destabilize both technological ecosystems and geopolitical environments.

A central insight that can be seen is the role of data, not merely as an input for AI functionality, but as a contested space. The integrity, control, and resilience of overall data will increasingly define the effectiveness and security of AI applications. When the data that trains and drives AI systems is vulnerable to manipulation, corruption, or theft, AI becomes not a strategic advantage, but a liability. The militarization of AI and its integration into critical infrastructure, particularly when combined with supply chain insecurities and open-source

diffusion, create an environment in which adversarial actors can exploit latent weaknesses far below the traditional thresholds of warfare.

Considering these findings, a number of key policy directions must be considered. First, there is a pressing need to strengthen the resilience of AI systems through robust data governance, secure and transparent supply chains, and ongoing testing for algorithmic integrity. Governments and institutions must develop capabilities for auditing, verifying, and stress-testing AI tools that operate in critical or dual-use contexts.

Second, ethical frameworks must move beyond voluntary principles and be embedded into legal, operational, and technical protocols. These frameworks should address not only the intended use of AI systems but also their potential misuse, ensuring that accountability mechanisms are preserved even as autonomy increases.

Furthermore, anticipatory governance must be prioritized through the integration of foresight practices into policy development. This includes funding scenario-based strategic planning, establishing early-warning mechanisms for emerging AI threats, and institutionalizing cross-sector dialogue between civilian innovators, military planners, and ethicists. Regulation should not aim to stifle innovation but rather to ensure that innovation does not outpace responsibility.

## BIBLIOGRAPHY


1. Borchert, H., Schütz, T., & Verbovszky, J. (Eds.). (2024). *The very long game: 25 case studies on the global state of defense AI*. Cham: Springer Nature Switzerland.
2. Brands, H., & Edel, C. N. (2019). *The lessons of tragedy: Statecraft and world order*. New Haven, CT: Yale University Press.
3. Cave, S., & Dihal, K. (2023). *Imagining AI: How the world sees intelligent machines*. Oxford: Oxford University Press.
4. Cave, S., Dihal, K., & Dillon, S. (Eds.). (2020). *AI narratives: A history of imaginative thinking about intelligent machines*. Oxford: Oxford University Press.
5. Csernatoni, R. (2024, July 17). Governing military AI amid a geopolitical minefield. Carnegie Europe. *Carnegie* [online]. URL: https://carnegieeurope.eu/2024/07/17/governing-military-ai-amid-geopolitical-minefield-pub-90731 [Accessed on April, 2025].
6. Fox, A.C. (2024, October). *Obstructive warfare: Applications and risks for AI in future military operations* (CIGI Paper No. 307). Waterloo, ON: Centre for International Governance Innovation.
7. Freedman, L. (2013). *Strategy: A history*. Oxford: Oxford University Press.
8. Fukuyama, F. (1992). *The end of history and the last man*. Florence, MA: Free Press.
9. Galdorisi, G., & Tangredi, S. J. (2024). *Algorithms of Armageddon*. Annapolis, Maryland: Naval Institute Press.
10. Hurbans, R. (2020). *Grokking artificial intelligence algorithms*. Shelter Island, NY: Manning Publications.
11. Johnson, J. (2022). The AI commander problem: Ethical, political, and psychological dilemmas of human-machine interactions in AI-enabled warfare. *Journal of Military Ethics.* 21(3–4). 246–271.
12. Johnson, J. (2023). *AI and the bomb: Nuclear strategy and risk in the digital age*. Oxford: Oxford University Press.
13. Mazzucchi, N. (2022). *AI-based technologies in hybrid conflict: The future of influence operations* (Hybrid CoE Paper 14). Helsinki: European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).
14. Miller, S. (2018). *Dual use science and technology, ethics and weapons of mass destruction*. Berlin: Springer.
15. Ong, T. (2021, January 22). EU adopts ethical guidelines for military use of artificial intelligence. *The Defense Post* [online]. URL: https://thedefensepost.com/2021/01/22/eu-ethics-military-ai/ [Accessed on April, 2025].
16. Pandya, J. (2019, January 7). The dual-use dilemma of artificial intelligence. *Forbes* [online]. URL:. https://www.forbes.com/sites/forbestechcouncil/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/ [Accessed on April, 2025].
17. Payne, K. (2021). *I, Warbot: The dawn of artificially intelligent conflict*. London: Hurst & Company.
18. Romele, A. (2023). *Digital habitus: A critique of the imaginaries of artificial intelligence* (1st ed.). London: Routledge.
19. Russell, S., & Norvig, P. (2020*). Artificial intelligence: A modern approach* (4th ed.). Hoboken, NJ: Prentice Hall.
20. Scharre, P. (2023). *Four battlegrounds: Power in the age of artificial intelligence*. New York: W.W. Norton & Company.
21. Simpson, K.H.; Paquette, S.; Racicot, R. & Villanove, S. (2025, February 26). Militarizing AI: How to catch the digital dragon? *Centre for International Governance Innovation*

*(CIGI)* [online]. URL: https://www.cigionline.org/articles/militarizing-ai-how-to-catch-the-digital-dragon/. [Accessed on April, 2025].
22. United Nations. (1945). *Charter of the United Nations and Statute of the International Court of Justice*. San Francisco: UN.
23. United Nations Security Council. (2021). *Final report of the Panel of Experts on Libya established pursuant to Security Council Resolution 1973 (2011)* (S/2021/229). New York: UN
24. Vaynman, J. & Volpe, T. A. (2023). Dual use deception: How technology shapes cooperation in international relations. *International Organization.* 77(3), 599–632. https://doi.org/10.1017/S0020818323000140.
25. Yan, G. (2020). The impact of artificial intelligence on hybrid warfare. *Small Wars & Insurgencies.* 31(4). 749–768. https://doi.org/10.1080/09592318.2019.1682908