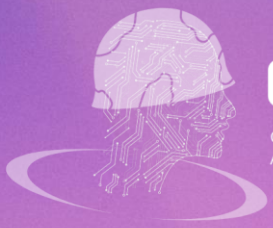

GC REAIM

GLOBAL COMMISSION ON RESPONSIBLE AI IN THE MILITARY DOMAIN

Foreign, Commonwealth & Development Office

GC REAIM Expert Policy Note Series

Applying International Law to AI in the Military Domain: An Integrated Approach

Fan Yang

April 2025

POWERED BY The Hague Centre for Strategic Studies

GC REAIM Expert Policy Note Series

Applying International Law to AI in the Military Domain: An Integrated Approach

Author: Fan Yang

April 2025

Cover photo: Unsplash

The Global Commission on Responsible Artificial Intelligence in the Military Domain (GC REAIM) is an initiative of the Government of the Netherlands that was launched during the 2023 REAIM Summit on Responsible Artificial Intelligence in the Military Domain in The Hague. Upon request of the Dutch Ministry of Foreign Affairs, the Hague Centre for Strategic Studies acts as the Secretariat of the Commission.

The GC REAIM Expert Policy Note Series was funded by the Foreign, Commonwealth and Development Office (FCDO) of the United Kingdom. GC REAIM Experts maintained full discretion over the topics covered by the Policy Notes. The contents of the GC REAIM Expert Policy Note series do not represent the views of the Global Commission as a whole. The Policy Notes are intended to highlight key issues related to the governance of AI in the military domain and provide policy recommendations.

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl

1. Introduction

Assessing the applicability of existing international law to artificial intelligence in the military domain (AIM) presents a complex challenge. The complexity arises from the diverse branches of international law involved and the inherently ambiguous nature of AI, which encompasses machine capabilities achieved through a combination of hardware and software that support essential elements of computational power, algorithms, and data. Attempting to address this complex question through a singular, universal analytical framework is impractical. One potential approach is to organize the analysis according to relevant branches of international law, such as *jus ad bellum*, *jus in bello*, international human rights law, the law of state responsibility, and international criminal law.[1] Alternatively, the analysis could be structured around the major stages in the life cycle of military AI, including its development, deployment, and utilization.[2] However, this note posits that a more pragmatic method is to disintegrate the international legal question into smaller components based on specific AIM scenarios, by focusing on key areas such as AI-driven lethal autonomous weapon systems (LAWS) and AI-empowered cyber operations, while also considering other AI-based military actions like AI-dependent influence operations or decision support systems (DSS). This 'integrated approach' would, *inter alia*, allow for the maximal incorporation of existing international discourse from both the academic and diplomatic arenas.

This note will first establish foundational premises to clarify the research question and analytical approach (Section 2). Subsequently, it will analyse the application of international law to key AIM scenarios: AI-driven LAWS (Section 3) and AI-empowered cyber operations (Section 4). After a brief examination of international legal issues related to other AIM scenarios (Section 5), the note will conclude with key findings and policy recommendations.

[1] Laura Bruun, Marta Bo, and Netta Goussac, 'Compliance with International Humanitarian Law in the Development and Use of Autonomous Weapon Systems: What Does IHL Permit, Prohibit and Require?' (SIPRI, March 2023), https://www.sipri.org/publications/2023/policy-reports/compliance-international-humanitarian-law-development-and-use-autonomous-weapon-systems-what-does.
[2] Sten Allik et al., 'A Framework for Human Decision-Making through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications', *A Framework for Human Decision-Making through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications*, October 2024, 1–63.

2. Foundational Premises

The applicability of existing international law to AIM has not encountered significant opposition. However, AI introduces challenges in regulating state behaviour concerning development and utilization of AI in the military domain, and in determining international legal responsibility. These challenges stem from two primary sets of factors. First, unpredictability and unexplainability. AI systems, particularly those based on data feeding and machine learning, inherently possess a degree of unpredictability and lack of transparency. This impacts the legal requirements for predictability and accountability, complicating the assessment of state actions involving AI in military contexts. Second, acceleration of decision-making processes. AI's capacity to rapidly collect and analyse information can significantly expedite decision-making processes. This acceleration may alter traditional decision-making chains, affecting legal evaluations and potentially challenging existing frameworks for accountability. These factors necessitate a revaluation of how relevant branches of international law apply to key scenarios of AIM, ensuring that legal standards effectively address the unique characteristics and implications of AI technologies in military applications.

2.1 Relevant Branches of International Law

This note focuses exclusively on existing international law (*lex lata*), namely those as recognized sources under Article 38 of the International Court of Justice (ICJ) Statute. Proposed non-binding norms or specific international rules under discussion (*lex ferenda*) are beyond the scope of this analysis. Nonetheless, various branches of international law are pertinent to the legal examination of state actions involving AI for military purposes.

First, general public international law establishes fundamental principles to facilitate peaceful coexistence among states and the resolution of disputes. Principles such as sovereignty, non-intervention, and due diligence delineate basic obligations when states engage in the development, deployment, and use of AI in the military domain. As the core principle of *jus ad bellum*, the prohibition of the use of force and its associated legal issue of the right to self-defence applies to AI in military contexts.

Second, the dual, human-centric international law branches – international human rights law (IHRL) and international humanitarian law (IHL) – aim to provide international legal protection over basic human rights against state actions involving AI, respectively in peacetime and during armed conflict.

Third, the issue of accountability is primarily addressed through the law of state responsibility and international criminal law. The former concerns potential state responsibility regarding AI in military applications arising from violations of primary international obligations, while the latter determines individual (especially commander) criminal responsibility for acts of international crimes resulting from the use of AI in military contexts.

Fourth, arms control law, including international treaties on arms trade, non-proliferation, and weapon control, is relevant for discussions on the development, export, or proliferation of AI-based weapon systems.

Beyond the aforementioned branches, other specific bodies of international law apply when the situation demands. For instance, the international legal status of AI-driven unmanned maritime vehicles (UMVs) and their engagement rules during armed conflict at sea are governed by the international law of the sea and the specific law of naval warfare. International environmental law is also of significant relevance, as the energy-intensive demands of military AI systems could aggravate resource scarcity and environmental degradation.

2.2 Key Scenarios of AI in the Military Domain

For the purpose of international legal analysis, adopting a reductionist approach by deconstructing the broad concept of AIM into specific scenarios proves beneficial. This method facilitates a more focused examination of how international law applies to each grand scenario and allows for the integration of existing international legal discourse pertinent to that specific context. Key application scenarios that AIM encompasses are AI-driven LAWS and AI-empowered cyber operations as well as AI-dependent influence operations and AI-based decision-support systems.

AI-driven LAWS represent a major subset of, if not an equivalent to, autonomous weapons systems capable of causing lethal consequences through the use of AI technology to automate functions such as target selection and engagement. The primary multilateral processes addressing LAWS include the Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts (GGE) on LAWS and the United Nations General Assembly First Committee Resolutions on LAWS. The central international legal issue concerning LAWS pertains to their compliance with IHL.[3]

Similarly, AI-empowered cyber operations for military purposes can be considered a subset of cyber operations.[4] Cyber operations encompass a wide range of offensive state activities utilizing Information and Communication Technology (ICT), including cyber theft, espionage, malign interruptive operations, and military cyber-attacks.[5] The integration of AI can significantly enhance the speed and scope of these operations. Key multilateral initiatives in this area include the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE) and its successor, the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International

[3] United Nations. *Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*. CCW/GGE.1/2019/3, 25 September 2019.
[4] Cyber operations should be distinguished from cyber-related measures, such as administrative regulation and enforcement measures on managing ICT supply chain, protecting internet infrastructure, enhancing cyber security, etc. Cyber operations are also different from network defence, as they respectively refer to operations outside vis-à-vis inside the cyberspace under the sovereign control of the acting state. See page 3 of United States. *Presidential Policy Directive 20: U.S. Cyber Operations Policy.* Washington, D.C.: The White House, 16 October 2012. Declassified and published by the National Security Archive. https://nsarchive.gwu.edu/sites/default/files/documents/2725521/Document-2-9.pdf.
[5] Angus King and Mike Gallagher, 'Cyberspace Solarium Commission - Report', 2020, https://www.solarium.gov/report.

Security (OEWG). While these processes focus on the application of international law in cyberspace, they do not necessarily emphasize the impact of AI. The use of AI in cyber operations introduces complexities related to attribution, proportionality, and the potential for unintended escalation, necessitating a more nuanced legal analysis to address these challenges.[6]

Compared to LAWS and cyber operations, it is a more recent phenomenon for military AI to enable influence operation in the form of cognitive warfare,[7] or to drive decision support systems in military targeting.[8] Both trigger intense legal debate as to potential breach of international obligations.

[6] Rain Liivoja, Maarja Naagel, and Ann Väljataga, 'Autonomous Cyber Capabilities under International Law', *NATO Cooperative Cyber Defence Centre of Excellence*, 2019, https://ccdcoe.org/library/publications/autonomous-cyber-capabilities-under-international-law/.

[7] Tsvetelina Benthem, Talita Dias, and Duncan Hollis, 'Information Operations under International Law', *Vanderbilt Journal of Transnational Law* 55, no. 5 (1 November 2022): 1217.

[8] Anna Nadibaidze, Ingvild Bode, and Qiaochu Zhang, 'AI in Military Decision Support Systems: A Review of Developments and Debates', Report, *AI in Military Decision Support Systems* (Odense: Center for War Studies, 4 November 2024).

3. Applying International Law to AI-driven LAWS

The application of international law to AI-driven LAWS covers all stages of the weapon system life cycle, including its development, testing, deployment, use, and assessment, each presenting distinct legal challenges. This analysis categorizes these challenges into three phases: before, during, and after an armed conflict that involves LAWS. While IHL plays a central role,[9] other branches such as arms control law, the law of state responsibility, and international criminal law are also pertinent.

3.1 Before Armed Conflict

Prior to deploying AI-driven LAWS, states are obligated under Article 36 of Additional Protocol I (AP I) of the Geneva Conventions to conduct a legal review, with LAWS being deemed as new weapons, means, or methods of warfare. Through a doctrinal reading of this article, the obligation is characterized as a duty of conduct, granting states some discretion in its implementation. Although some have proposed to establish a more stringent and legally-binding multilateral mechanism for the review of LAWS,[10] such a proposal is still inchoate. A few legal technical questions are yet to be clarified, which can be grouped under two primary themes. The first theme regards the scope of issues to cover in the review. For example, it is debatable whether to include for the legal review merely the development of LAWS prototypes, or also later iterations; merely the hardware, or also the software component, or even its training dataset. The second theme regards the applicable rules that serve as the benchmarks for the review. Here the debate revolves around a central question: if the use of a weapon is inconsistent with provisions of other international law than IHL, should that weapon be considered as failing the Article 36 legal review?

Another prominent international legal issue at this stage concerns potential trade of AI-driven LAWS. The Arms Trade Treaty (ATT) plays a central role as it provides a framework for regulating the international trade of conventional arms. Under Article 6 of the ATT, states are prohibited from transferring arms that would be used to commit genocide, crimes against humanity, or war crimes. Additionally, Article 7 requires states to assess the risk of such transfers contributing to violations of IHL or human rights law. The unique capabilities of AI-driven LAWS raise complex questions regarding their classification under the ATT. Specifically, there is a need to determine whether AI software integral to these systems qualifies as "parts and components" under Article 4

[9] The CCW GGE already affirmed, in adopting possible guiding principles in 2018, that IHL applies to all weapon systems including LAWS, see United Nations. *Report of the 2018 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems.* CCW/GGE.1/2018/3, 23 October 2018. https://documents.un.org/doc/undoc/gen/g18/323/29/pdf/g1832329.pdf.

[10] Japan. *Possible Outcome of 2019 GGE and Future Actions of International Community on LAWS.* Working paper CCW/GGE.2/2019/WP.3, submitted to the Group of Governmental Experts on Lethal Autonomous Weapons Systems, Convention on Certain Conventional Weapons, 2019. https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2019/gge/Documents/GGE.2-WP3.pdf.

of the ATT, thereby subjecting it to export controls. Given the potential dual use of AI software, the legal interpretation has to give due account to those who may want to use it for peaceful purposes.

3.2 During Armed Conflict

During an armed conflict, the deployment of AI-driven LAWS is governed primarily by IHL rules on the conduct of hostilities. Analysing the legality of each tactical military operation can be facilitated by differentiating between the planning and execution phases.

In the planning phase, IHL mandates the belligerent state to carefully define the military objective and select the means and methods of attack, to avoid or minimize collateral damage to civilians. If AI-driven LAWS are to be employed to achieve a specific military objective, several factors affecting human control over the weapon system should be evaluated to ensure compliance with IHL. Measures may include setting temporal, geographical, and payload limitations for the LAWS, maintaining communication links to preserve the option of human override when necessary, and broadcasting early warnings when possible. All these steps help demonstrate that human combatants and fighters have conducted the requisite IHL calculations, in a way that accommodates AI characteristics, to balance military necessity with humanitarian considerations.

During the execution phase, though presumably operating within the operational limitations established during the planning phase and encoded into the system, AI-driven LAWS may possess a certain degree of autonomy to adapt to field conditions. This autonomy presents significant challenges for IHL, particularly concerning the distinction between combatants and non-combatants. AI systems may struggle to accurately identify individuals *hors de combat* or those directly participating in hostilities, potentially leading to violations of the principle of distinction. Additionally, ensuring that the use of lethal force remains proportionate to the anticipated direct military advantage may be too complex of a decision for autonomous systems to make. Even if future AI technology can ensure the LAWS perform at an equal or even superior level to humans, legal and ethical barriers persist regarding the delegation of life-and-death decisions to machines.

3.3 After Armed Conflict

After an armed conflict involving the use of LAWS, the primary international legal issue is accountability, especially when the deployment and use of LAWS potentially violated IHL obligations. This concern translates into two legal assessments: state responsibility and individual responsibility.

To establish state responsibility, there must be a breach of primary international law—specifically, IHL rules governing the conduct of hostilities—and a legal attribution of the wrongful act to the responsible state. This also includes situations where a state deploys LAWS that have not been adequately tested or reviewed prior to deployment, thus violating its obligation of legal review; or where a state exports AI-driven LAWS inconsistently with its obligations under applicable arms control law.

Determining individual responsibility for human combatants and fighters presents legal complexities. International criminal law requires a mental element (*mens rea*) for war crimes, typically at the level of *dolus directus* of the second degree[11] or at least *dolus eventualis*.[12] Applying these standards to the use of AI-driven LAWS is challenging, as the autonomous nature of these systems may obscure the intent and knowledge of the individuals involved. If this legal barrier is not addressed, it would hinder the implementation of the CCW GGE guiding principle that "accountability cannot be transferred to machines".[13]

Before concluding this section, three additional considerations merit attention. First, IHL, through its Martens Clause, provides a framework that bridges legal norms and ethical considerations. This ensures that concerns regarding LAWS, which may not be explicitly addressed by existing IHL, are subject to ethical scrutiny.[14]

Second, the legal assessment of LAWS compliance with IHL is often context-dependent. Before reaching a definitive legal conclusion, several factors must be considered, including the specifications and features of the weapon system, the operational environment, and the nature of the assigned task. Only through this nuanced approach can it be ensured that legal evaluations are tailored to the specific circumstances of each deployment.

Third, AI-driven LAWS operating at sea, such as unmanned maritime vehicles (UMVs), invoke specific bodies of international law, including the United Nations Convention on the Law of the Sea (UNCLOS) and the *lex specialis* of naval warfare. Determining whether such UMVs qualify as 'ships' or 'warships'[15] and identifying the specific obligations they must observe during naval engagements[16] require careful legal analysis within these frameworks.

---

[11] International Criminal Court. *Prosecutor v. Katanga*, ICC-01/04-01/07, Judgment, 17 March 2014, para. 294.
See also International Criminal Court. *Prosecutor v. Bemba*, ICC-01/05-01/08, Judgment, 21 March 2016, para. 52.

[12] International Criminal Tribunal for the former Yugoslavia. *Prosecutor v. Mucić et al.* (Čelebići Case), IT-96-21-T, Judgment, 16 November 1998, para. 160.

[13] United Nations. *Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*. CCW/GGE.1/2019/3, 25 September 2019.

[14] ICRC, 'Ethics and Autonomous Weapon Systems: An Ethical Basis for Human Control? | International Committee of the Red Cross', 2019, 3 April 2018, https://www.icrc.org/en/document/ethics-and-autonomous-weapon-systems-ethical-basis-human-control.

[15] Simon McKenzie, 'When Is a Ship a Ship? Use by State Armed Forces of Un-Crewed Maritime Vehicles and the United Nations Convention on the Law of the Sea', *University of Queensland Law School*, 2020, https://doi.org/10.31228/osf.io/a7xtc.

[16] Michael Schmitt and David Goddard, 'International Law and the Military Use of Unmanned Maritime Systems', International Review of the Red Cross, 15 August 2016, http://international-review.icrc.org/articles/international-law-and-military-use-unmanned-maritime-systems.

4. Applying International Law to AI-empowered Cyber Operation

4.1 Evolving Debate of International Law on Cyber Operation

How the nature of 'cyber operations' is understood has undergone a paradigm shift[17] over the past two decades. Earlier cyber power theory saw cyber operations primarily as a new form of military force.[18] Recent schools of thought interpret cyber operation as a strategic campaign that generates maximized yield by persistently engaging with adversaries;[19] as more of an 'intelligence contest' than a military contest;[20] or as an understudied yet well-used instrument of power: subversion.[21] These recent doctrines converge on characterizing the severity of cyber operations as below the threshold of armed conflict, whose features cannot be captured by the language of war studies.

Simultaneous within this process are constant verbal battles on the potential (un)lawfulness of cyber operations in diplomatic and academic fora. A similar change of focus can also be witnessed in related international law literature. Aligned with the notion of cyber power theory, earlier treatises predominantly unfold from the perspective of *jus ad bellum* and *jus in bello*.[22] After realizing that there is a wide spectrum of cyber operations, publicists broadened their discussion to cover other themes of international rules in peacetime, particularly the law of state responsibility.[23] Recent

[17] Jacquelyn Schneider et al., 'Ten Years In: Implementing Strategic Approaches to Cyberspace', *Newport Papers*, 1 January 2020, https://digital-commons.usnwc.edu/usnwc-newport-papers/45.
[18] Joseph Nye, 'Cyber Power | The Belfer Center for Science and International Affairs', 2010, https://www.belfercenter.org/publication/cyber-power.
[19] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford University Press, 2022).
[20] Joshua Rovner, 'Cyber War as an Intelligence Contest', War on the Rocks, 16 September 2019, http://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/; for more detailed discussion see: Robert Chesney et al., 'Policy Roundtable: Cyber Conflict as an Intelligence Contest', Texas National Security Review, 17 September 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.
[21] Lennart Maschmeyer, 'Subversion, Cyber Operations, and Reverse Structural Power in World Politics', *European Journal of International Relations* 29, no. 1 (1 March 2023): 79–103, https://doi.org/10.1177/13540661221117051; Lennart Maschmeyer, 'A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict', *Journal of Strategic Studies* 46, no. 3 (16 April 2023): 570–94, https://doi.org/10.1080/01402390.2022.2104253.
[22] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge Studies in International and Comparative Law (Cambridge: Cambridge University Press, 2012), https://doi.org/10.1017/CBO9780511894527; Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), https://doi.org/10.1017/CBO9781139169288; Marco Roscini and Leverhulme Trust, *Cyber Operations and the Use of Force in International Law* (OUP Oxford, 2014).
[23] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524; François Delerue, *Cyber Operations and International Law*, Cambridge Studies in International and Comparative Law

publications began to adopt a more focused approach to the (un)lawfulness of a specific sub-category of cyber operations.[24]

4.2 AI-specific Challenges to International Law on Cyber Operation

If cyber operations were to be empowered by AI to an unseen before scale and efficiency,[25] specific international legal challenges may arise. These challenges manifest in four key dimensions:

First, AI's capacity to mimic human behaviour patterns, forge code signatures, and automate obfuscation mechanisms undermines conventional forensic techniques. This may worsen "attribution deficiency" as states struggle to conclusively link attacks to specific actors. The proliferation of open-source AI tools further complicates matters by enabling non-state actors to execute sophisticated operations. This may potentially obscure state involvement through proxy relationships or technical outsourcing.

Second, current interpretations of Article 2(4) of the UN Charter, which ties the prohibition of force to physical consequences, become inadequate when addressing AI-augmented cyber operations. Attacks causing systemic collapse of power grids or financial systems—without direct physical destruction—challenge the binary distinction between "armed attack" and non-kinetic coercion. This ambiguity further destabilizes the legal foundations for self-defence under Article 51, particularly given AI's capacity for rapid, cross-border attack propagation.

Third, existing international law lacks mechanisms to address distributed responsibility in AI-enabled attacks involving multinational supply chains (e.g., one state's algorithms deployed through another's hardware). The autonomous decision-making capabilities of machine learning systems create further dilemmas: when AI independently escalates attack strategies, current doctrines struggle to determine whether such actions constitute deliberate state actions or technical anomalies.

Fourth, the technical disparity between AI-capable states and those lacking defensive infrastructure risks entrenching a "cyber deterrence hierarchy", where dominant powers weaponize AI superiority while weaker states face systemic vulnerabilities. This imbalance is exacerbated by divergent national cybersecurity regulations, which hinder real-time evidence sharing and coordinated responses to transnational AI attacks.

(Cambridge: Cambridge University Press, 2020), https://doi.org/10.1017/9781108780605; Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press, 2020), https://doi.org/10.1017/9781108807050.

[24] Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart, 2019); Peter B. M. J. Pijpers, *Influence Operations in Cyberspace and the Applicability of International Law*, 1st ed., Elgar International Law and Technology Series (Northampton: Edward Elgar Publishing, 2023).

[25] Matthew Giannelis, 'AI-Powered Cyber Attacks - The Alarming 85% Global Surge', Tech Business News, 4 April 2024, https://www.techbusinessnews.com.au/blog/ai-driven-cyber-attacks-the-alarming-surge/.

5. Applying International Law to AI-empowered Cyber Operation

5.1 AI-dependent Influence Operation under International Law

Influence operations are characterized by the core tenets of "(a) the absence of the use of force or even warfare; (b) the focus on the cognitive dimension; and (c) the objective to change the behaviour of other actors directly or indirectly via a change in attitude".[26] While traditionally employed during peacetime for political ends, influence operations can also serve as supplementary means in armed conflict to deceive or disorganize the opposing party, in synergy with kinetic or cyber military operations. AI has the potential to revolutionize the landscape of influence operations,[27] as deceitful content can be generated and distributed with unprecedented low cost and high efficiency, and generative AI is more likely to evade content moderation and security checks designed to filter unwanted information.

The international legal challenges posed by AI-dependent influence operations in the military domain are twofold. First, determining whether such operations amount to prohibited intervention is complex. Existing international rules require the operation to target a reserved domain and include an element of 'coercion'.[28] These criteria may be difficult to apply to AI-dependent influence operations, which can subtly and covertly alter public opinion without direct coercion. Second, there is the question of how international human rights law can ensure the protection of the right to be informed and freedom of speech in an environment saturated with AI-generated information. The rapid proliferation of AI-generated content poses significant challenges to the integrity of information ecosystems worldwide.

5.2 AI-based Decision Support Systems under International Law

Another AIM scenario, which is occasionally discussed and relatively understudied, is the AI-based decision support systems (DSS). Unlike LAWS, DSS would not autonomously engage in the use of force, but could support military personnel in decision-making, including for targeting. Scrutinizing DSS under existing international law requires a close examination of its AI characteristics such as data feeding and algorithmic deduction,

[26] Peter B. M. J. Pijpers, *Influence Operations in Cyberspace and the Applicability of International Law*, 1st ed., Elgar International Law and Technology Series (Northampton: Edward Elgar Publishing, 2023).
[27] OpenAI, 'Disrupting Deceptive Uses of AI by Covert Influence Operations', 2024, https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/.
[28] International Court of Justice. *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America).* Merits, Judgment, 27 June 1986, para. 205.

which primarily engender IHL concerns.[29] Based on the well-recognized significance of maintaining human agency in military targeting, the involvement of human decision-makers is essential for the interpretation and application of IHL, especially in complex, context-sensitive situations like proportionality assessments. AI-based DSS may undermine this human agency by producing outputs that lack the necessary contextual and qualitative legal judgment required by IHL. Moreover, the reliance on machine learning, which is characterized by opacity, biases, and limited reliability, would only worsen the deficit in making legal evaluations of proportionality in warfare.

[29] Taylor Kate Woodcock, 'Human/Machine(-Learning) Interactions, Human Agency and the International Humanitarian Law Proportionality Standard', *Global Society*, 2 January 2024, https://www.tandfonline.com/doi/abs/10.1080/13600826.2023.2267592; Henning Lahmann, 'Self-Determination in the Age of Algorithmic Warfare', *European Journal of Legal Studies* 16 (2025): 161–214, https://doi.org/10.2924/EJLS.2025.LT.005.

6. Conclusion

This short policy note has three preliminary findings. First, there is no one-size-fits-all solution for practically applying existing international law to address AI-specific risks and needs in the military domain. Second, various branches of international law, when paired with the major scenarios of AIM, can form a useful matrix for structured analysis, as is reflected in the annexed Table 1. Third, despite the recent hype in debates on military AI, a considerable part of international legal challenges remains traditional legal questions, rather than being AI-specific. In other words, how the element of AI actually affects international legal analysis invites more in-depth analysis.

In light of these findings, the note concludes with three policy recommendations:

1. Recognize AI-driven Lethal Autonomous Weapon Systems (LAWS) and AI-empowered cyber operations as the two key pillars of AIM, and adopt an integrated approach in the study of applying international law to AIM. Engaging with the ongoing international law debates revolving around the two themes, both in relevant multilateral processes and academic dialogues, is the most practical approach to enhance the international community's understanding of applying international law to AIM.
2. The GC REAIM can serve as a platform to cross-check international legal analyses arising from different AIM scenarios. Through this process, more AI-specific risks can be identified, and the most practically effective approaches to addressing such risks within specific branches of international law can be assessed.
3. Conduct context-dependent examinations to enable legal assessments that delve into nuanced aspects, ensuring that analyses are tailored to the specific circumstances of a given AIM scenario.

Appendix

	Main sources	Purpose	Exemplified relevance to AIM
Basic principles of international law	• UN Charter • Customary International Law • Judicial decisions by international tribunals	to set the fundamental principles of the international society for states to peacefully coexist and settle disputes	would the legal examination of use of AI for military purpose amounting to breach of sovereignty or non-intervention make any difference?
Jus ad bellum	• UN Charter, especially Arts. 2(4) & 51 • Customary International Law • Judicial decisions by international tribunals	to govern the use of force by States as an instrument of their national policy	would deployment of AI capability activate the right to (preventive) self-defence, as it would more likely constitute an 'imminent threat' of armed attack?
Jus in bello, or international humanitarian law	• Geneva Conventions • Customary IHL rules • Judicial decisions by international tribunals	to protect the victims of armed conflicts, international or non-international, and to regulate hostilities based on a balance between military necessity and humanity	would the development of AIM be subject to legal review according to IHL? would the deployment or use of AIM in armed conflict violate key IHL principles?
International human rights law	• Multilateral or regional human rights treaties • Customary International Law • Judicial decisions by international human rights tribunals	to ensure the legal protection of individual citizens' human rights against states during peace times	would the state's development of AIM inherently violate its obligation to protect human rights?
Law of state responsibility	• DARSIWA (as compiled by ILC) • Customary International Law	to define international wrongful acts and possible remedies the injured state can resort to	would the development or use of AIM, or arms trade thereof, be deemed as inconsistent with applicable primary international rules and incur state responsibility?
International criminal law	• Rome Statute • Customary International Law • Judicial decisions by international criminal tribunals	to determine individual especially commander criminal responsibility for acts of international crimes	would the deployment or use of AIM in armed conflict be deemed as an act of war crime and incur commander's criminal responsibility, especially with possible legal barrier on the element of *mens rea*?

Arms control law	• International treaties on arms trade, anti-proliferation, and weapon control	to impose international restrictions upon the development, production, stockpiling, proliferation and usage of small arms, conventional weapons, and weapons of mass destruction	would the export of AIM weapon system be in violation of applicable arms trade treaty?
Other specific body of international law e.g. international law of the sea	• UNCLOS • Customary International Law (as reflected in the Sanremo Manual) • Judicial decisions by international tribunals	to define the legal status of maritime vehicles and their accompanied rights and obligations, and to impose engagement rules for armed conflict at sea	would AI-enabled unmanned maritime vehicle enjoy the legal rights under the status of 'ships' or 'warships'?

Annex Table 1: Branches of International Law Relevant to AIM

Bibliography

Benthem, Tsvetelina, Talita Dias, and Duncan Hollis. 'Information Operations under International Law'. *Vanderbilt Journal of Transnational Law* 55, no. 5 (1 November 2022): 1217.

Bruun, Laura, Marta Bo, and Netta Goussac. 'Compliance with International Humanitarian Law in the Development and Use of Autonomous Weapon Systems: What Does IHL Permit, Prohibit and Require?' SIPRI, March 2023. https://www.sipri.org/publications/2023/policy-reports/compliance-international-humanitarian-law-development-and-use-autonomous-weapon-systems-what-does.

Delerue, François. *Cyber Operations and International Law*. Cambridge Studies in International and Comparative Law. Cambridge: Cambridge University Press, 2020. https://doi.org/10.1017/9781108780605.

Lahmann, Henning. 'Self-Determination in the Age of Algorithmic Warfare'. *European Journal of Legal Studies* 16 (2025): 161–214. https://doi.org/10.2924/EJLS.2025.LT.005.

Mačák, Kubo. 'Unblurring the Lines: Military Cyber Operations and International Law'. *Journal of Cyber Policy*, 2 September 2021. https://www.tandfonline.com/doi/abs/10.1080/23738871.2021.2014919.

McFarland, Tim. 'Factors Shaping the Legal Implications of Increasingly Autonomous Military Systems'. International Review of the Red Cross, 21 November 2016. http://international-review.icrc.org/articles/factors-shaping-legal-implications-increasingly-autonomous-military-systems.

Nadibaidze, Anna, Ingvild Bode, and Qiaochu Zhang. 'AI in Military Decision Support Systems: A Review of Developments and Debates'. Report. *AI in Military Decision Support Systems*. Odense: Center for War Studies, 4 November 2024.

Pijpers, Peter B. M. J. *Influence Operations in Cyberspace and the Applicability of International Law*. 1st ed. Elgar International Law and Technology Series. Northampton: Edward Elgar Publishing, 2023.

'Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems', 2019.

Sweijs, Tim, and Sofia Romansky. 'International Norms Development and AI in the Military Domain'. Working Paper. CIGI Papers, 2024. https://www.econstor.eu/handle/10419/303159.

UN Secretary-General. 'Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security : Budget Implications of Draft Resolution A/C.1/79/L.43 :: Statement /: Submitted by the Secretary-General in Accordance with Rule 153 of the Rules of Procedure of the General Assembly', 28 October 2024. https://digitallibrary.un.org/record/4065062.

Woodcock, Taylor Kate. 'Human/Machine(-Learning) Interactions, Human Agency and the International Humanitarian Law Proportionality Standard'. *Global Society*, 2 January 2024. https://www.tandfonline.com/doi/abs/10.1080/13600826.2023.2267592.

About the Author

Dr. Fan Yang

Dr. Fan Yang is an Assistant Professor of international law at Xiamen University (China), currently also Visiting Associate Fellow at the Hague Program of International Cyber Security, Leiden University. He is the initiator and Deputy Director of Cyberspace International Law Center, Xiamen University School of Law; Deputy Director of International Economic Law Institute of Xiamen University; Executive Editor of Chinese Journal of International Economic Law. He is actively involved in a series of Track 1.5 and Track 2 dialogues on international governance concerning emerging and disruptive technologies, including especially serving as the liaison and expert for Sino-EU Expert Working Group on the Application of International Law in Cyberspace.

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies