

Building Defence Capabilities for Future Uncertainty

Edited by

Laurenz Fürst · Ugurhan Berkok

David Last · Odin Bartsch



Building Defence Capabilities for Future Uncertainty

Edited by
Laurenz Fürst, Ugurhan Berkok, David Last and Odin Bartsch

NATO DEEP eAcademy
International Society of Military Sciences, and
Swedish Defence University

2026

Cover image: developed by Copilot from composite images.

Building Defence Capabilities for Future Uncertainty

First published 2025 by NATO DEEP eAcademy Press

Uniwersytet Warmińsko-Mazurski w Olsztynie ul. Michała Oczapowskiego 2 10-719 Olsztyn, Poland

and the Polish Association for Security and War Studies University of Poland, (Akademia Sztuki Wojennej) al. gen. Antoniego Chruściela “Montera” 103 00-910 Warsaw-Rembertów, Poland.

This publication is part of the Defence Education Enhancement Programme (DEEP) series inspired by collaboration with the International Society of Military Sciences (www.isofms.org)

The content of this publication does not reflect the official opinion of the North Atlantic Treaty Organization or other official positions of organizations associated with its publication or its contributors. Responsibility for the information and views expressed in this book lies entirely with the authors and the editors.

ISBN: 978-83-975616-3-2

Reviewers:

Assoc. Prof. Piotr Gawliczek, PhD

COL Assoc. Prof. Andrzej SOBOŃ, PhD, Eng.

© 2025 selection and editorial matter, Laurenz Fürst, Ugurhan Berkok, David Last, Odin Bartsch. Individual chapters, the contributors.

The right of Laurenz Fürst, Ugurhan Berkok, David Last and Odin Bartsch to be identified as the authors of the editorial material, and of the authors for their individual chapters has been asserted in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

This work, *Building Defence Capabilities for Future Uncertainty*, edited by Laurenz Fürst, Ugurhan Berkok, David Last, and Odin Bartsch, is licenced under Creative Commons Attribution NonCommercial ShareAlike Licence 4.0 by NATO DEEP eAcademy Press and the War Studies University of Poland.

You are free to share, copy and redistribute the material in any medium or format. The licensor cannot revoke these freedoms as long as you follow the licence terms:



Attribution – You must give appropriate credit and provide a link to the licence.



Non-commercial – You may not use the material for commercial purposes.



No Derivatives – If you remix, transform, or build upon the material you may not distribute the modified material.

No additional restrictions – You may not apply legal terms or technological measures that restrict others from doing anything the licence permits.

Figures	ix
Tables	xi
Contributors	xii
Acknowledgement	xxii
Foreword	xxiii
List of Abbreviations	xxv
Introduction: Conflict Today and the Uncertainty of Future Wars, David Last	xxx
Section 1: Strengthening Domestic Defence	xl ix
Chapter 1: Integrating Human Rights and Emerging Technologies in Defence Capabilities: A Framework for Ethical Resilience, Marco Marsili	1
Chapter 2: Approaches to Assess Troop's Resilience in Defense, Oleksandr Maistrenko.....	19
Chapter 3: The legal challenges in the protection of submarine cable, Ahmed Abdel Hakam.....	37
Chapter 4: Robustness of Tactical and Military Networks Against Natural Disasters and Hostile Environments: A Comprehensive Analysis of Military Communication Systems Resilience, Abdellah Chehri and Dorota Domalewska.....	58
Chapter 5: The role and legal status of military intelligence in combatting hybrid threats, Eerik Heldna	90
Section 2: Modernization of Military Capabilities	109
Chapter 6: Forming an Analytic Framework for the Communication of the Military Utility of Technology, Kent Andersson and Patrik Stensson	110
Chapter 7: The impact of hybrid threats on operations in modern warfare.	130
Chapter 8: Do Drones Dream of Transparent Battlefields? Dealing with Past and Future Alternatives to the Tactical Crisis in Contemporary Warfare, Sandro Teixeira Moita.....	146
Chapter 9: Negotiation as a Key Enabler Behind Multi-Domain Operations, Pedro B. Àgua, Vitor Conceição, and Anacieto Correia	157
Chapter 10: A Contemporary Taxonomy of Information Warfare: An Analysis Proposal Based on Scientific Production, Mariana Grilli Belinotte and Luiz Rogério Franco Goldoni.....	172
Chapter 11: The Significance of News as an Aspect of Information Operation in the South China Sea Conflict, Bagus Jatmiko, Marseito, and Irhamni Ali	203
Chapter 12: Building EU defense capabilities for energy-tech hybrid warfare from Russia and China, Maurizio Geri.....	224
Chapter 13: Wargaming Tomorrow's Threats: Fostering Critical Thinking Through Simulation-Based Learning, Tali Neumann	237
Chapter 14: Geopolitical Futures and Force Structure Planning, Robert Addinall, Ali Dizboni, and Peter Gizewski	250
Chapter 15: Terrorism in Armed Conflicts: A Breach of Norms or an Element of Strategic Culture as per Example of the Russian Federation and Soviet Union, Maria Juczewska	262

Section 1: Strengthening Domestic Defence

Chapter 1: Integrating Human Rights and Emerging Technologies in Defence Capabilities: A Framework for Ethical Resilience

Dr. Marco **Marsili**, ORCID: <https://orcid.org/0000-0003-1848-9775>

Abstract:

As the global security landscape becomes increasingly complex and unpredictable, the need for robust defence capabilities that are both effective and ethically sound is paramount. This paper explores the intersection of human rights, emerging technologies, and defence capabilities, arguing that future military strategies must integrate ethical considerations to ensure resilience in an uncertain future. The rapid advancement of technologies such as artificial intelligence, cyber capabilities, and autonomous systems presents both opportunities and challenges for national security. While these technologies can enhance operational effectiveness, they also raise significant ethical concerns regarding privacy, accountability, and the potential for misuse. Among these, lethal autonomous weapon systems represent a particularly contentious area, as they challenge established norms of human control and responsibility in armed conflict. This paper proposes a framework for building defence capabilities that prioritize human rights and ethical standards, aiming to mitigate the risk that technological advancements may erode fundamental freedoms. The discussion will focus on three key areas: what capabilities should be built, who will build them, and how they will be built. It will advocate for a collaborative approach involving governments, international organisations, and civil society to develop guidelines and best practices that align defence strategies with human rights principles. By fostering a culture of ethical resilience, this paper aims to contribute to the discourse on sustainable defence capabilities that not only address immediate security needs but also uphold the values of democracy and human dignity in an increasingly volatile world.

Keywords: Human Rights Integration, Ethical Resilience, Accountability Frameworks, Ethical Standards, Military Ethics

Introduction

Technological innovations are redefining the global security landscape, creating unprecedented opportunities alongside significant risks. Emerging technologies such as artificial intelligence [AI], autonomous systems, and cyber capabilities are transforming the nature of conflict and military operations. However, this transformation does not come without consequences for human rights, raising pressing questions about the adequacy of existing

international frameworks in addressing these challenges. In this context, fostering ethical resilience becomes paramount to ensuring that technological innovation aligns with fundamental rights and democratic values.

Defence capabilities cannot be assessed solely in terms of efficiency or technological advancement; they must also be evaluated against their compatibility with fundamental principles of human dignity and justice. As highlighted in earlier studies (Marsili, 2022), contemporary military strategies often operate in ambiguous environments below the threshold of conventional armed conflict, underscoring the need for a robust and adaptable normative framework. This concern is well-established in the literature on civil wars and human rights, where scholars such as DeRouen and Heo (2007), Kalyvas (2006), and Weinstein (2007) have examined how irregular and fragmented conflict environments challenge the applicability of international legal norms and complicate efforts to protect civilians and uphold human rights.

Building on prior work examining dual-use innovation and decentralized AI governance (Marsili, 2025a; 2025b), this paper proposes a normative and operational framework aimed at aligning emerging military technologies with ethical and human rights standards. This contribution argues that integrating human rights into defence strategies is not merely a moral imperative but a practical necessity for ensuring long-term stability and security. In response to the inadequacies of existing normative frameworks, the concept of 'ethical resilience' is proposed as a strategic and conceptual tool to reconcile technological innovation with the preservation of universal values. By engaging in key theoretical perspectives and drawing on relevant case studies, the paper outlines a normative and operational framework for the development of ethical defence capabilities capable of addressing the complexities of contemporary and future conflict environments.

While emerging technologies encompass a broad and diverse array of innovations, this contribution does not aim to examine each category in detail. Instead, it focuses primarily on lethal autonomous weapon systems [LAWS], which present particularly acute ethical and legal challenges within the broader technological landscape.¹

Key Concepts

In examining the intersection of military ethics, lethal autonomous weapon systems, and human rights, it is essential to first define key terms that will underpin the discussion: defence capabilities, human rights, and ethical resilience. Defence capabilities refer to the technological, strategic, and operational capacities that military forces develop to ensure national security. These

¹ For a detailed definition of emerging technologies, a discussion on how they differ from disruptive technologies, and a comprehensive list, see Marsili (2023a, pp. 25, 26, 32).

capabilities are increasingly influenced by the rapid development of advanced technologies, particularly those incorporating artificial intelligence and automation. Human rights, in the context of warfare, are principles designed to protect individuals from state violence, ensuring that military operations do not infringe upon the fundamental rights and dignity of persons, particularly civilians (Ruggie, 2011). Ethical resilience is the ability of a military force or defense system to adapt and respond to new technologies in a manner that aligns with ethical and human rights standards, even as the nature of conflict evolves (Marsili, 2025a).

The advent of LAWS raises significant ethical questions, particularly regarding the delegation of life-and-death decisions to machines. As previously discussed, (Marsili, 2023a), military disruptive technologies, including autonomous weapon systems, create a significant risk of delegating life-and-death decisions to machines without adequate ethical oversight. This raises profound ethical implications about whether machines can truly adhere to moral principles and whether humans should entrust such decisions to algorithms. This concern has been further explored by Marsili (2024), who applies the Autonomy Spectrum Framework to real-world systems, highlighting the legal and ethical dilemmas posed by delegating lethal decisions to autonomous technologies.

As these systems become more capable, they challenge traditional notions of human agency in warfare. Autonomous weapons, which can identify, select, and engage targets without direct human intervention, introduce complexities in accountability and proportionality, requiring a new ethical approach (Marsili, 2025a), two key principles of international humanitarian law (Crootoof, 2018; Sharkey, 2019). The primary concern is that, while LAWS may enhance operational efficiency, they may also erode the human element in warfare, increasing the risk of violations of human rights (Sharkey, 2019).

In response to these challenges, scholars argue that the ethical use of LAWS requires more than just adherence to existing legal frameworks; it requires the development of an ethical resilience within military strategies (Anderson & Waxman, 2017). This involves integrating ethical considerations into the design, deployment, and usage of LAWS, ensuring that these systems operate in a way that respects human dignity and comply with the principles of international law (Scharre, 2018). The application of human rights in defence strategies, therefore, demands that states and international actors carefully consider the implications of technological advancements and establish robust safeguards to prevent abuses.

John Ruggie's concept of social purpose within the framework of business and human rights also provides valuable insight for the military context. Ruggie argues that businesses must respect human rights and ensure that their operations do not cause harm, a principle that can be

extended to the defense sector (Ruggie, 2011; 2013). This notion of social purpose in military technologies suggests that defence capabilities must not only be designed for strategic superiority but must also serve the broader goal of safeguarding human dignity and minimizing harm.

As military technologies evolve, too must the strategies that govern their deployment. The integration of human rights into defence capabilities is not merely a legal obligation but a necessary ethical practice, particularly in light of recent developments in AI and digital autonomy (Marsili, 2025b). The military sector must build ethical resilience to adapt to the changing landscape of warfare, ensuring that new technologies such as LAWS do not undermine international legal standards or infringe upon fundamental human rights (Marsili, 2022; Scharre, 2018).

Another critical factor shaping ethical decision-making in defence is the cultural relativity of how societies perceive acceptable military casualties. While democratic states may be constrained by political and public intolerance toward high loss of life, authoritarian regimes may be more willing to accept—or even conceal—substantial losses in pursuit of tactical objectives. This divergence in ethical calculus has profound implications for the implementation of human rights standards in asymmetric or hybrid conflicts.

Legal and Ethical Implications of Lethal Autonomous Weapons Systems

The deployment of autonomous weapons systems in modern warfare raises profound legal and ethical challenges, particularly regarding compliance with international humanitarian law [IHL] and international human rights law [IHRL]. LAWS—systems capable of independently identifying, targeting, and engaging military objectives—threaten to alter the nature of warfare, introducing new concerns about accountability, proportionality, and distinction between combatants and civilians (Crootoof, 2018).

There are legal obligations and ethical considerations associated with the use of LAWS in military operations, as well as broader implications for human rights and ethical resilience. International humanitarian law, particularly the *Geneva Conventions* and their *Additional Protocols*, governs the conduct of warfare and aims to minimize the suffering of those involved in or affected by armed conflict. These principles require that all military actions comply with the core tenets of distinction, proportionality, and necessity (Scharre, 2018). The principle of distinction demands that parties to a conflict distinguish between combatants and civilians, targeting only legitimate military objectives. However, the implementation of LAWS in warfare presents significant challenges to this principle, as these systems must be capable of distinguishing between lawful and unlawful targets under complex and dynamic battlefield conditions (Crootoof, 2018). The autonomy of these systems raises concerns about the accuracy

and reliability of such distinctions, particularly when LAWS are deployed in complex environments where the identification of civilians and non-combatants becomes more difficult.

The principle of proportionality, which prohibits attacks that may cause excessive harm to civilians or the natural environment in relation to the anticipated military advantage, is similarly jeopardized by LAWS. For instance, the use of fully autonomous drones in complex urban environments—such as those hypothetically envisioned in future autonomous strike missions—raises serious concerns about the system's ability to assess proportionality in real time, particularly where civilians are intermingled with combatants (Sparrow, 2007; Human Rights Watch, 2012). Critics argue that LAWS, lacking human judgment and empathy, may struggle to make nuanced assessments of proportionality in rapidly evolving combat scenarios (Sharkey, 2019). As autonomous systems are increasingly integrated into military strategies, the capacity for humans to intervene in targeting decisions diminishes, leading to fears of disproportionate harm and the erosion of accountability.

Additionally, the challenge of accountability remains paramount in the discussion of LAWS. Under existing IHL frameworks, accountability for violations of international law, such as unlawful killings or war crimes, typically falls upon human actors, whether military commanders or political leaders. However, as decision-making shifts to machines, the responsibility for violations becomes increasingly opaque, raising questions about whether and how accountability can be assigned (Anderson & Waxman, 2017). While LAWS may operate within the confines of IHL, legal scholars argue that further clarification is needed regarding the responsibility of the human operators and commanders who deploy them (Crootoft, 2018). This ambiguity has led to calls for new frameworks and specific regulations that address the unique characteristics of autonomous systems in warfare.

The ethical implications of LAWS extend beyond legal concerns, involving a broader discourse on the morality of delegating life-and-death decisions to machines. Marsili and Wróblewska-Jachna (2024) highlight how the rapid developments in AI technology, such as deep learning, have led to an increased pervasiveness and proliferation of misinformation through deep fakes. This calls for a focus on international standards and policy measures to enhance the trustworthiness of AI systems.

Ethical theorists have raised serious concerns about the potential erosion of human dignity and the accountability of military forces engaged in combat (Scharre, 2018). One significant ethical challenge is the potential loss of human control over the application of force, which has traditionally been viewed as essential to preserving the ethical integrity of military operations (Sharkey, 2019).

According to John Ruggie's framework on business and human rights, the ethical use of technology—whether in the business or military domain—requires that systems be designed

with human rights protection at their core, ensuring that these technologies do not lead to harm (Ruggie, 2011; 2013). By extension, in the military context, the use of LAWS must be balanced by ensuring that these systems respect the rights and dignity of civilians and combatants alike. This includes ensuring compliance with IHL, while also considering the broader humanitarian impact of deploying such systems in conflict zones.

Ethical concerns regarding autonomy in warfare are also reflected in debates surrounding the moral implications of 'killer robots'. Critics argue that by allowing machines to make life-and-death decisions, societies risk undermining the human capacity for empathy, which is often considered essential to ethical decision-making in warfare (Sharkey, 2019). While LAWS may be capable of executing military strategies with precision, they lack the ability to weigh the broader ethical consequences of their actions in the way a human commander might. This moral agency, which involves the capacity to reflect on the consequences of one's actions and adapt to the complexities of warfare, is a core argument against the development and use of fully autonomous weapon systems.

The growing integration of LAWS also prompts reflection on the ethical resilience of military institutions in adapting to such technologies. Ethical resilience entails the ability of military organizations to adapt their strategies, tactics, and operational frameworks to integrate advanced technologies without compromising human dignity or the principles of international law (Anderson & Waxman, 2017). Military leadership must engage in ongoing ethical reflection, ensuring that technological advancements are aligned with fundamental human rights and international humanitarian principles.

Emerging Technologies and Their Implications

Emerging technologies are rapidly redefining modern defence by blurring the boundaries of conventional warfare and introducing new operational domains. Artificial intelligence, autonomous weapons, and cyber capabilities not only enhance military effectiveness but also disrupt established norms governing accountability, human oversight, and the lawful use of force. These developments challenge the principles of proportionality and distinction, shifting the character of armed conflict and raising urgent questions about the adequacy of existing legal and ethical frameworks.

One of the most significant innovations is the development of autonomous weapon systems, which can select and engage targets without human intervention. As highlighted by Scharre (2018), LAWS have the potential to increase operational efficiency and reduce human casualties, but they also introduce risks such as accountability gaps, lack of human judgement,

and the possibility of malfunction or unintended escalation. Autonomous systems could, for instance, make decisions in high-stakes combat situations where human emotions, biases, and ethical considerations could play a crucial role. Scharre (2018) argues that the challenge lies in ensuring that these systems comply with international humanitarian law, particularly the principles of distinction and proportionality, which require that military operations distinguish between combatants and civilians, and avoid excessive harm to civilians relative to the military advantage gained. Marsili's paper on LAWS (2024) discusses how these autonomous systems pose serious ethical dilemmas around the dehumanisation of warfare and the need for robust legal frameworks to ensure accountability and human oversight drawing on the dynamic autonomy model to propose a flexible approach that calibrates machine autonomy based on contextual complexity and humanitarian risk. The contribution advocates for stronger international regulations to ensure LAWS are used in compliance with ethical standards. Similarly, Crootof (2018) highlights how LAWS could lower the threshold for initiating armed conflicts, especially when integrated with AI systems capable of analyzing vast amounts of data and making rapid decisions, thus increasing the speed of warfare and potentially reducing opportunities for diplomatic intervention.

Artificial intelligence, which underpins many of these autonomous systems, also introduces new dimensions to warfare. As Crootof (2018) discusses, the deployment of AI in warfare may inadvertently lower the threshold for conflict initiation and escalation, particularly in cyber warfare and remote combat scenarios. Complementing this perspective, Zweibelson (2025) argues for a reconceptualization of warfare itself, emphasizing the need to understand conflict as a dynamic, multi-domain phenomenon influenced by technological disruption and shifting geopolitical realities. The ease of using AI for offensive operations can make it more likely for states to engage in conflicts without fully considering the long-term humanitarian consequences. Additionally, AI-driven systems raise concerns about the opacity of decision-making processes, as these technologies may not be easily understandable to human operators, making it difficult to attribute responsibility for errors or violations of IHL (Marsili, 2023a).

Cyber capabilities are another emerging technology that significantly impacts modern warfare. While cyber operations can be used to enhance national security and disrupt enemy systems, they also pose risks to civilian infrastructure and human rights. Attacks on critical infrastructure such as power grids, healthcare systems, or communication networks could have devastating effects on civilian populations. Moreover, the anonymity and low-cost nature of cyber warfare make it a particularly attractive option for non-state actors and rogue states, further complicating the global security environment. As highlighted in the literature, cyber warfare lacks clear rules of engagement, which raises questions about the legality of certain actions under

international law, particularly when it comes to attacks that have a direct impact on civilians (Ruggie, 2011).

While emerging technologies offer significant advantages in terms of military effectiveness, their implications for human rights are profound. As warned (Marsili, 2022), there is a growing need for comprehensive frameworks that can balance technological advancements with respect for international human rights standards. The risks of using autonomous systems and AI-driven technologies in military contexts include not only violations of IHL but also potential abuses of power by authoritarian regimes, who could leverage these technologies for surveillance, repression, and control over populations. This underscores the importance of ensuring that the development and deployment of these technologies are guided by robust ethical considerations and international cooperation.

The importance of establishing ethical guidelines and frameworks for emerging technologies in defence is further emphasized in studies examining their broader impact. As scholars continue to investigate the intersection between emerging technologies and human rights, it is critical that their development and use in warfare be continuously assessed to ensure that they adhere to international norms. The potential for states to abuse technologies such as AI and autonomous weapons underscores the need for effective oversight and governance (Sharkey, 2019). Furthermore, international collaboration will be necessary to develop a shared understanding of how these technologies should be used, ensuring that ethical resilience is maintained even as technological capabilities evolve.

To summarise, while emerging technologies have the potential to enhance defence capabilities, they also introduce significant risks. The challenge is to navigate the fine line between leveraging these innovations for military advantage and safeguarding human rights and ethical standards. The rapid evolution of AI, cyber capabilities, and autonomous systems is reshaping the strategic and operational landscape of modern defence, presenting profound ethical and legal challenges. These technologies blur traditional boundaries of warfare, complicating accountability and the protection of human rights. As discussed earlier, concerns around proportionality, distinction, and human control are central to understanding their impact. Against this backdrop, the concept of ethical resilience emerges as a vital framework to guide the responsible development and deployment of these innovations. As we move forward, it is crucial that discussions around such technologies remain anchored in the broader imperatives of human dignity, accountability, and compliance with international law, ensuring that technological progress aligns with the fundamental principles that safeguard society.

The increasing complexity of modern warfare, particularly in hybrid environments, further complicates the application of international humanitarian law. Hybrid threats, including cyber operations, disinformation, and proxy warfare, challenge the enforcement of accountability and the protection of civilians. As recent conflicts have shown, state and non-state actors alike may deliberately exploit the legal and ethical constraints observed by democratic societies, perceiving them as operational weaknesses. This underscores the importance of developing ethical resilience not only in relation to technological systems, but also to evolving strategic doctrines (Kaldor, 2012).

Ethical Resilience in Defence Capabilities

As military technologies evolve, ensuring their ethical integration within national defence strategies is paramount. The concept of 'ethical resilience' refers to the ability to adapt military strategies to rapidly advancing technologies while maintaining a commitment to core human rights principles. This involves a multifaceted approach to not only managing risks but also fostering a culture of accountability and ethical decision-making within defence institutions. The development of autonomous weapon systems, artificial intelligence, and cyber capabilities presents a unique challenge in this regard, requiring careful consideration of how these technologies are regulated and employed in military contexts.

The importance of ensuring that these technologies are not misused or employed irresponsibly is highlighted by scholars such as Crootof (2018), who contend that LAWS could radically shift the traditional understanding of accountability in warfare. Without proper oversight, these systems could make autonomous decisions that violate established ethical norms, leading to unintended harm or violations of international humanitarian law. Furthermore, Scharre (2018) underscores the importance of maintaining human oversight in such systems, as human judgement remains crucial in interpreting the complex moral and legal dimensions of warfare—an issue also highlighted by Christian (2020), who warns that even the most advanced AI systems struggle to internalize nuanced human values and ethical reasoning.

The growing reliance on AI in military decision-making processes poses significant questions about autonomy, accountability, and responsibility. Marsili's proposal (2023a) emphasizes the importance of integrating human rights considerations into the development and deployment of emerging military technologies like AI and autonomous systems. This includes maintaining human oversight, establishing accountability mechanisms, and fostering international cooperation to regulate these technologies within the bounds of international law and human rights principles.

In scenarios where human operators are physically or mentally disconnected from decision-making, the ethical implications become even more pronounced. As Sharkey (2019) notes, the delegation of life-and-death decisions to machines challenges fundamental ethical and legal frameworks, including principles of proportionality and necessity, central tenets of IHL. Thus, ensuring ethical resilience requires continuous oversight and adaptation of IHL to account for new technologies that blur the line between human and machine decision-making.

The issue of ethical resilience is further compounded by the use of cyber warfare tactics. The growing use of cyberattacks as a means of conducting warfare or influencing the geopolitical landscape presents a challenge to traditional ethical and legal frameworks. As Marsili (2023b) discusses, cyber capabilities can affect civilian infrastructures, potentially violating principles of distinction and proportionality under IHL. The integration of these technologies must thus be accompanied by comprehensive frameworks that ensure compliance with human rights standards, with a focus on transparency and accountability.

In response to these challenges, international legal scholars such as Ruggie (2011) have emphasized the importance of guiding principles for the integration of emerging technologies in military contexts. His work on business and human rights stresses that all technological advancements, particularly those used in defence, must adhere to ethical standards that protect fundamental human rights, ensuring that the pursuit of technological and strategic advantages does not come at the expense of moral obligations.

This ethical framework should be considered not as a static set of rules but as a dynamic and evolving set of principles that adapt to new challenges and threats. As such, ensuring ethical resilience in defence capabilities involves not only adhering to established international law but also anticipating and addressing future ethical dilemmas posed by emerging technologies. The key lies in promoting a balanced approach—one that leverages technological advancements for national security while simultaneously safeguarding the rights and dignity of individuals affected by these developments.

Legal and Regulatory Frameworks for Ethical Resilience in Emerging Military Technologies

The integration of emerging technologies, particularly in the realm of autonomous weapons systems and artificial intelligence, necessitates a robust legal and regulatory framework to ensure ethical resilience. This framework should address not only the operational aspects of these technologies but also the broader ethical, legal, and humanitarian challenges they pose. A key component of this framework is the adherence to existing international laws such as international humanitarian law, international human rights law, and various arms control treaties. However, as

the nature of warfare evolves with these new technologies, there is an increasing need to adapt and potentially expand these legal frameworks.

One of the primary concerns regarding the deployment of LAWS is ensuring compliance with the core principles of IHL, which include distinction, proportionality, and necessity. These principles require that military operations must distinguish between combatants and non-combatants, that the force used in combat must be proportionate to the military objective, and that force must only be used when necessary. Scharre (2018) argues that LAWS could potentially undermine these principles by operating with minimal human oversight, leading to unintentional civilian harm or disproportionate use of force. To mitigate these risks, Scharre (2018) suggests that strict accountability mechanisms and ongoing human oversight are essential to maintaining compliance with IHL.

Moreover, the issue of autonomy in military technologies raises significant legal questions about responsibility and accountability. As noted by Crootof (2018), when LAWS operate autonomously, they blur the lines of responsibility for their actions. Traditional legal frameworks assume that human agents are responsible for the actions of military technologies, but with the increasing autonomy of these systems, it becomes unclear who should be held accountable in the event of unlawful or unethical actions. To address this, Crootof (2018) suggests that international law must evolve to explicitly account for autonomous systems, ensuring that their use is regulated and that clear chains of responsibility are established.

In addition to IHL, international human rights law plays a crucial role in ensuring that military technologies do not violate fundamental human rights, particularly the right to life, liberty, and security. The United Nations *Guiding Principles on Business and Human Rights* (Ruggie, 2011) provides a framework for ensuring that all actors, including military organizations, respect human rights in the context of technological development and deployment. These principles emphasize the need for companies and governments to ensure that technologies, such as LAWS and AI systems, do not contribute to human rights abuses, including unlawful killings or violations of privacy.

Ruggie's (2013) work on multinational corporations and human rights further highlights the responsibility of private actors, such as defense contractors, in ensuring that their technologies are developed and deployed in a manner consistent with international human rights standards. This responsibility extends to ensuring that AI and other autonomous technologies used in military contexts are designed to minimize harm to civilians and avoid violations of fundamental rights.

Finally, the rapid development of AI in warfare raises significant challenges in terms of arms control and regulation. The potential for AI to be weaponized, as discussed by Sharkey (2019),

presents new challenges in regulating military technologies. Sharkey (2019) suggests that a global ban on autonomous weapons might be an ideal solution, but the practicalities of such a ban are fraught with difficulties, including the potential for states to circumvent regulations by developing technologies in secret or for non-state actors to use them. Instead, Sharkey (2019) advocates for robust international agreements that focus on controlling the use of autonomous weapons and AI in military operations while ensuring that they are used in accordance with established legal and ethical standards.

Ultimately, the legal and regulatory frameworks that govern the use of emerging military technologies must evolve to address the unique challenges posed by LAWS and AI. These frameworks should ensure that the principles of IHL, human rights law, and international arms control are adhered to, while also promoting ethical resilience through oversight, accountability, and international cooperation.

Analysis of Current Challenges and Opportunities

The integration of emerging technologies in military defense systems presents both significant opportunities and formidable challenges. The rapid advancement of artificial intelligence, autonomous weapon systems, and cyber capabilities has led to new paradigms in warfare, while simultaneously raising complex ethical, legal, and strategic issues. These technologies promise enhanced military effectiveness, precision, and the ability to conduct operations in more dynamic and unpredictable environments. However, they also bring substantial risks, particularly in relation to the preservation of human rights, the accountability of decision-makers, and the potential for unintended consequences.

A major challenge in the adoption of emerging technologies in defense is the alignment of technological capabilities with existing legal frameworks, particularly international humanitarian law. The use of autonomous weapons systems, for example, introduces concerns about compliance with principles such as distinction (*the ability to differentiate between combatants and non-combatants*) and proportionality (*ensuring the response is proportional to the threat*). The introduction of AI-driven systems in military contexts further complicates accountability and transparency, raising questions about who is responsible in the event of a malfunction or misuse (Anderson & Waxman, 2017; Scharre, 2018). Legal scholars argue that while some autonomous systems could potentially adhere to IHL standards, ensuring compliance at the operational level is far from guaranteed.

The absence of universally accepted frameworks to regulate these technologies underscores the gap between rapid technological development and existing regulatory

mechanisms. Many international bodies and scholars are calling for preemptive regulation or even bans on certain types of autonomous weapons to prevent potential abuses (Sharkey, 2019). However, as Anderson and Waxman (2017) highlight, a blanket ban on AI in warfare could stifle technological progress and limit the potential military advantages that could arise from these innovations.

Human rights concerns are another critical dimension in the deployment of emerging technologies in defense. Autonomous systems, especially those capable of lethal force, pose risks to human dignity and could undermine the protection of civilian life. Technologies like AI-driven drones or robotic soldiers challenge the traditional notions of human oversight in lethal decision-making. Ruggie (2011; 2013) emphasizes the importance of a framework that ensures businesses (*or in this case, military contractors*) and governments adhere to human rights standards, aligning military innovations with principles of justice and the protection of human life.

As emerging technologies increasingly influence military operations, ensuring that these technologies respect international human rights standards are crucial. The development of AI-driven defense systems must consider not only the military objectives but also the broader societal implications of autonomous decision-making in conflict, including the potential for escalation or misuse in authoritarian regimes (Marsili, 2022). The challenge lies in designing systems that retain human oversight while enhancing operational efficiency.

Despite these challenges, emerging technologies also present strategic opportunities that could significantly alter the landscape of defense. AI, for instance, could provide a more accurate and faster decision-making process, improve military capabilities while reducing the risk to human soldiers. Autonomous systems could also enhance the ability to conduct operations in complex environments, such as urban warfare or in regions with high levels of contamination, where human intervention might be impractical or too dangerous (Crootof, 2018; Scharre, 2018).

In addition, the integration of cyber capabilities into military defense has the potential to revolutionize warfare. Cyber-attacks can disrupt enemy communications, disable critical infrastructure, or gather intelligence without the need for traditional kinetic operations (Marsili, 2023b). These capabilities could offer a significant strategic advantage in situations where traditional warfare methods are less effective or impossible to use. The challenge, however, remains in ensuring that these capabilities are used ethically and within the bounds of international law.

The primary opportunity lies in balancing technological advancements with ethical responsibility. As Scharre (2018) suggests, achieving a balance between military power and human rights is fundamental. Technologies must be developed with an awareness of their potential

consequences, ensuring that the deployment of autonomous and AI-driven systems does not erode the core ethical principles that govern warfare. To navigate these challenges, it is essential to establish clear ethical guidelines and regulatory frameworks that guide the development, deployment, and use of emerging technologies in defense.

Moreover, as emerging technologies continue to evolve, it is essential for policymakers and military leaders to adopt a proactive approach to ethical resilience. This involves anticipating the potential risks and designing systems that are adaptable to future challenges, ensuring that defense capabilities remain robust while safeguarding human dignity and rights.

The integration of emerging technologies into military defense systems offers significant opportunities to enhance operational efficiency and effectiveness. However, these advancements must be carefully balanced with the ethical, legal, and human rights considerations that underpin modern warfare. By addressing the challenges and opportunities outlined above, the international community can ensure that technological advancements in defense contribute to greater security without undermining the fundamental values that govern warfare.

Strategic Recommendations for Integrating Human Rights and Emerging Technologies in Defense

The integration of emerging technologies into military defense systems offers numerous strategic benefits but also presents significant ethical and operational challenges. In order to harness the potential of artificial intelligence, autonomous weapons systems, and other disruptive technologies while safeguarding human rights, it is essential to develop comprehensive strategies that balance technological advancement with legal and ethical obligations. As argued (Marsili, 2024), future international regulatory efforts must ensure meaningful human control, especially in high-risk scenarios where civilian protection is paramount.

One of the first steps in ensuring that emerging technologies are used responsibly in defense is the establishment of clear ethical guidelines and legal frameworks. These frameworks should be built on existing international humanitarian law and human rights law while adapting to the specific challenges posed by autonomous systems and AI. Anderson and Waxman (2017) argue that while a ban on autonomous weapons might be unrealistic, it is crucial to shape the development of such systems in ways that ensure compliance with IHL principles such as proportionality and distinction.

To guide this process, governments and international bodies must engage in multi-stakeholder dialogues, including defense experts, ethicists, human rights advocates, and policymakers. These discussions should focus on creating common standards that can be applied

globally, ensuring that the deployment of autonomous systems respects fundamental human rights and remains consistent with military ethics.

Despite the potential for AI and autonomous systems to improve military capabilities, it is vital to retain human oversight in decision-making processes, particularly in the use of lethal force. As Scharre (2018) suggests, human control is essential to ensure that military operations remain aligned with ethical norms and legal standards. This could be achieved through hybrid systems where AI assists decision-making, but final judgments are made by human commanders.

Moreover, accountability mechanisms should be put in place to track the actions of autonomous systems and their operators. These mechanisms could include real-time monitoring of AI behavior, transparent auditing processes, and clear lines of accountability for any actions that result in violations of human rights or IHL.

Given the global nature of technological advancements and the potential for emerging technologies to be deployed across borders, fostering international cooperation is essential. Ruggie (2011) stresses the importance of the "Protect, Respect, and Remedy" framework, which guides the actions of both states and private companies in ensuring respect for human rights. For defense technologies, this framework can help ensure that military applications do not undermine human dignity or violate the rights of individuals, especially civilians caught in conflict zones.

The proliferation of private military companies [PMCs] and the widespread use of proxy forces further erode the traditional understanding of state monopoly on legitimate force. These actors, often operating outside the scope of international law, engage in combat operations without the same legal or ethical obligations as regular armed forces. This fragmentation of responsibility complicates the attribution of violations and weakens enforcement mechanisms for human rights and humanitarian law (Singer, 2003).

International agreements should be pursued to establish common norms and standards for the use of autonomous and AI-driven systems in military operations. These norms could include restrictions on the development and deployment of fully autonomous lethal systems and encourage transparency in the use of AI technologies.

Another key recommendation is the integration of human rights considerations into military strategy and training. As technologies evolve, it is essential that military personnel are educated on the ethical implications of these technologies. Training should include scenario-based exercises where military operators learn to navigate the ethical dilemmas posed by autonomous systems, ensuring they understand their responsibilities under IHL and human rights law.

Incorporating human rights into military strategy is not just about compliance; it is also about ensuring that military operations contribute to long-term peace and stability. As Marsili (2023b)

points out, ethical military practices are essential not only for legal compliance but for maintaining the legitimacy of military operations in the eyes of the global community.

Finally, defense technologies should not only be developed with a focus on combat efficiency but also with the aim of preventing conflicts and de-escalating tensions. AI and autonomous systems can be used to improve intelligence gathering, enhance early warning systems, and support peacekeeping missions by reducing the need for human intervention in high-risk areas.

However, the development of such technologies must be approached cautiously. As Sharkey (2019) warns, the increased reliance on autonomous systems could lead to unforeseen consequences, such as the escalation of conflicts or the inadvertent targeting of civilian populations. Therefore, adaptive technologies should prioritize conflict prevention and de-escalation capabilities to ensure that military engagement remains a last resort.

The integration of emerging technologies in defense offers significant potential for enhancing operational capabilities and improving strategic outcomes. However, these technologies must be deployed in a way that upholds human rights and adheres to ethical standards. By establishing clear legal frameworks, ensuring human oversight, fostering international cooperation, and prioritizing human rights in military strategy, it is possible to create a defense system that is both advanced and ethically resilient.

Conclusion

In conclusion, integrating human rights principles within emerging defence technologies is essential for ensuring their ethical deployment. As military capabilities increasingly incorporate advanced technologies such as artificial intelligence and autonomous systems, it becomes crucial to maintain a balance between their operational advantages and the protection of fundamental human rights. Proactive frameworks that prioritize accountability, transparency, and international law can ensure these technologies are developed and used responsibly.

By embedding human rights into military technology development, we can mitigate risks like accountability gaps and the potential for disproportionate harm. Moreover, as the nature of warfare continues to evolve with technologies like AI, cyber capabilities, and hybrid warfare, decision-makers must consider both technological advancements and ethical standards. Ensuring that innovations in military capabilities align with human rights will be vital for maintaining global stability, peace, and security in the face of future challenges. Thus, fostering a defence framework that is both resilient and ethically sound is critical to navigating the complexities of modern warfare.

References

- Anderson, K., & Waxman, M.C. (2013). *Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can*. Stanford University, The Hoover Institution (Jean Perkins Task Force on National Security and Law Essay Series), American University, WCL Research Paper 2013-11, Columbia Public Law Research Paper 13-351. <http://dx.doi.org/10.2139/ssrn.2250126>.
- Christian, B. (2020). *The Alignment Problem: Machine Learning and Human Values*. W.W. Norton & Company.
- Crootof, R. (2018). Autonomous Weapon Systems and the Threshold of Armed Conflict. *International Law Studies*, 94, 210–249.
- DeRouen, K., & Heo, U. (2007). *Civil Wars of the World: Major Conflicts since World War II* (Vols. 1–2). ABC-CLIO.
- Human Rights Watch. (2012). *Losing Humanity: The Case Against Killer Robots*. <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>
- Kaldor, M. (2012). *New and Old Wars: Organized Violence in a Global Era* (3rd ed.). Polity Press.
- Kalyvas, S.N. (2006). *The Logic of Violence in Civil War*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511818462>.
- Marsili, M. (2022). Hybrid Warfare: Above or Below the Threshold of Armed Conflict?. *Hungarian Defence Review (Honvédségi Szemle)*, 150(1-2).
- Marsili, M. (2023a). Military Emerging Disruptive Technologies: Compliance with International Law and Ethical Standards. In Kalpokas, I., & Kalpokienė, J. (Eds.), *Intelligent and Autonomous: Transforming Values in the Face of Technology* (pp. 25-50). Value Inquiry Book Series (VIBS), Vol. 390. Brill. https://doi.org/10.1163/9789004547261_004.
- Marsili, M. (2023b). Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse. *Applied Cybersecurity & Internet Governance (ACIG)*, 2(1), 1–11. <https://doi.org/10.60097/ACIG/162861>.
- Marsili, M. (2024). Lethal Autonomous Weapon Systems: Ethical Dilemmas and Legal Compliance in the Era of Military Disruptive Technologies. *International Journal of Robotics and Automation Technology*, 11, 63–68. <https://doi.org/10.31875/2409-9694.2024.11.05>.
- Marsili, M. (2025a). Emerging and Disruptive Technologies: Strategic Implications and Ethical Challenges of Dual-Use Innovations. *Strategic Leadership Journal. Challenges for Geopolitics and Organizational Development*, 1, 57–71. <https://doi.org/10.5281/zenodo.15305895>.
- Marsili, M. (2025b). DeGen Artificial Intelligence: Challenges and Opportunities of AI Applications. *European Cybersecurity Journal (ECJ)*, 10(1), 67–80. <https://doi.org/10.5281/zenodo.15198603>.
- Marsili, M., & Wróblewska-Jachna, J. (2024). Digital Revolution and Artificial Intelligence as Challenges for Today. *Media i Społeczeństwo*, 20(1), 19–30. <https://doi.org/10.5604/01.3001.0054.6506>.
- Ruggie, J.G. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. New York, NY: United Nations. <https://digitallibrary.un.org/record/720245?v=pdf>.
- Ruggie, J.G. (2013). *Just Business: Multinational Corporations and Human Rights*. W.W. Norton & Company.
- Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. W.W. Norton & Company.
- Sharkey, A. (2019). Autonomous Weapons Systems, Killer Robots and Human Dignity. *Ethics Inf Technol*, 21, 75–87. <https://doi.org/10.1007/s10676-018-9494-0>.

Singer, P.W. (2003). *Corporate Warriors: The Rise of the Privatized Military Industry*. Cornell University Press.

Weinstein, J.M. (2007). *Inside Rebellion: The Politics of Insurgent Violence*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511808654>.

Zweibelson, B. (2025). *Reconceptualizing War*. Helion & Company.