CLARA BRAGA DE SOUSA

Unpacking the Notion of "Meaningful Human Control" in the Regulation of Autonomous Weapon Systems

Dissertation to obtain a Master's Degree in Law,
in the specialty of Law and Security.

Supervisor:

Dr. Laura Íñigo Álvarez, Professor at the NOVA School of Law

2025 SEPTEMBER

NOVA SCHOOL OF LAW

Declaração antiplágio

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

(Nome e assinatura do/a aluno/a)

Clara Braga de Sousa 

Anti plagiarism statement

I hereby declare that the work I present is my own work and that all my citations are correctly acknowledged. I am aware that the use of unacknowledged extraneous materials and sources constitutes a serious ethical and disciplinary offence.

(Student's name and signature)

Clara Braga de Sousa 

DEDICATION

To my loved ones, whose support, encouragement, and understanding have been a constant source of strength throughout this journey.

ACKNOWLEDGMENTS

I would like to begin by expressing my sincere gratitude to Dr. Laura Íñigo Álvarez, Professor at the NOVA School of Law and my thesis supervisor, for her invaluable guidance, intellectual insight, and constant encouragement throughout the course of this research. Her mentorship has been a continuous source of inspiration. Having first been my professor during the Master's in Law and Security at NOVA School of Law, she introduced me to International Humanitarian Law and was instrumental in sparking my interest in the regulation of Autonomous Weapon Systems. I am deeply thankful for the opportunity she gave me to pursue this topic, and for the trust and support that have enabled me to grow both academically and personally.

My sincere appreciation also goes to the NOVA School of Law for providing me with an intellectually rigorous and supportive academic environment. The curriculum of the Master's in Law and Security has been fundamental in shaping my academic path. In particular, it has enabled me to engage with contemporary legal challenges and to approach the complex questions of international law with both rigor and creativity. This program has been essential in equipping me with the analytical tools and perspectives necessary to undertake this research.

To my colleagues, some of whom became dear friends, I am equally grateful. In particular, I am thankful to Teresa and Melika for their companionship, insightful discussions, and unwavering support. Sharing this academic journey with them has made the experience not only more enriching but also deeply meaningful.

Finally, I express my heartfelt gratitude to my family, friends, and my partner, Mikael. To my family, for their endless patience, belief, and encouragement, especially during the most demanding stages of this journey. To Mikael, for his constant love, support, and understanding, which have been a continuous source of strength and balance throughout.

Declaration that the body of the thesis, including spaces and notes, occupies a total of **208292** characters.

Table of Contents

Introduction.....1

Methodology.....4
Research Question.....5

Chapter 1. Frameworks of Control: Defining the Intersection of IHL Principles and AWS....9

1.1. Autonomous Weapon Systems and IHL: Core Principles and Modern Challenges.....10
1.2. Assessing AWS Human Oversight through Legal and Academic Perspectives.....14
1.3. Concluding Remarks.....20

Chapter 2. Human Oversight in Autonomous Warfare: Ethical, Legal, and Operational Imperatives.....21

2.1. Safeguarding Humanity: The Crucial Role of Human Oversight in AWS.....22
2.2. Stakeholder Responsibilities and Challenges in Implementing MHC over AWS.....25
2.3. Navigating Operational Challenges in AWS: Implementing MHC for Ethical and Legal Alignment.....29
2.4. Concluding Remarks.....36

Chapter 3. From Supervision to Responsibility: Building the Foundations of MHC in AWS 37

3.1. Ensuring Human Oversight: Supervision, Authorization, and Accountability in AWS....38
3.2. Operationalizing Context Control and Decision-Making in AWS: Bridging Strategic Oversight with Tactical Precision.....44
3.3. Building Responsibility and Trust Through Oversight and Transparent Command in AWS Operations.....49
3.4. Concluding Remarks.....55

Conclusion – Moving Forward in the Pursuit of a Definition of MHC.....56

4.1. Core Components of MHC: Transparency, Accountability, and Technical Standards.....57
4.2. Refining the CCW GGE Rolling Text through the Lens of MHC.....61
4.3. From Norms to Practice: Navigating the Political Realities of Treaty Operationalization 71
4.4. Concluding Remarks.....75

Abstract

This thesis seeks to critically examine and define the concept of "Meaningful Human Control" (MHC) in the regulation of Autonomous Weapon Systems (AWS), an area of growing importance but persistent ambiguity in both legal and academic discourse. Through an in-depth analysis of key principles embedded in IHL – Proportionality, Distinction, and Military Necessity – this research will explore the ethical, legal, and operational dimensions of human oversight in AWS deployment. As AWS technology continues to evolve at an unprecedented pace, the absence of a universally accepted definition of MHC poses significant challenges to accountability, compliance with IHL, and the preservation of humane agency in life-and-death decisions. The study delves into the legal and ethical dilemmas as well as the practical difficulties of retaining meaningful human involvement in AWS operations, particularly in the context of increasingly autonomous systems. It draws on real-world examples, such as autonomous drones' swarms and Ukraine's AI-driven military drones, to illustrate the current gaps in regulation and the risks of unchecked technological proliferation. By analyzing the role of human control in these scenarios, this thesis proposes key elements necessary for meaningful human oversight, including human supervision, accountability mechanisms, and contextual control over AWS actions. Furthermore, the research outlines a potential international treaty framework to govern the use of AWS, ensuring that technological advancements in warfare are balanced with ethical responsibility and legal compliance. The proposed framework emphasizes the need for international cooperation, accountability, and stringent safeguards to prevent arms races and misuse of AWS. Ultimately, this thesis offers concrete recommendations for integrating human control into future legal frameworks, addressing the urgent need for clarity in defining what constitutes "meaningful" human oversight in the age of autonomous warfare.

Keywords

Autonomous Weapon Systems, Meaningful Human Control, International Humanitarian Law, Proportionality, Distinction, Accountability, Artificial Intelligence

Resumo

Esta tese propõe uma análise aprofundada do conceito de "Controle Humano Significativo" (CHS) na regulamentação dos Sistemas de Armas Autônomas (SAA), um tema de crescente relevância, ainda permeado por ambiguidades tanto no debate jurídico quanto no acadêmico. Explorando os princípios centrais do Direito Internacional Humanitário (DIH) – Proporcionalidade, Distinção e Necessidade Militar –, a pesquisa busca compreender as implicações éticas, jurídicas e operacionais do controle humano sobre os SAA. Com o desenvolvimento acelerado dessas tecnologias, a ausência de uma definição universalmente aceita de CHS levanta questões prementes de responsabilização, conformidade com o DIH e preservação da dignidade humana em decisões de vida ou morte. O estudo aborda dilemas éticos e legais, assim como as dificuldades práticas de manter uma supervisão humana eficaz na operação de SAA, especialmente em sistemas de autonomia crescente. Exemplos concretos, como enxames de drones autônomos e drones militares movidos por IA na Ucrânia, são usados para ilustrar as lacunas na regulamentação e os riscos de uma proliferação tecnológica descontrolada. Ao explorar o papel do controle humano nesses cenários, esta tese identifica elementos essenciais para uma supervisão significativa, incluindo a supervisão direta, mecanismos de responsabilização e controle contextual sobre as ações dos SAA. Ademais, a pesquisa propõe uma estrutura para um tratado internacional que regulamente o uso de SAA, garantindo que os avanços tecnológicos no campo bélico sejam equilibrados por uma responsabilidade ética e pelo respeito às normas legais. Tal estrutura enfatiza a importância da cooperação internacional, da responsabilização e de rigorosas salvaguardas para impedir corridas armamentistas e o uso indevido dos SAA. Em última análise, esta tese oferece recomendações concretas para integrar o controle humano nos futuros marcos jurídicos, destacando a urgência de uma definição clara do que constitui um controle humano "significativo" na era da guerra autônoma.

Palavras-chave

Sistemas de Armas Autônomas, Controle Humano Significativo, Direito Internacional Humanitário, Proporcionalidade, Distinção, Responsabilização, Inteligência Artificial, Drones

Introduction

The rapid development and deployment of AWS are significantly transforming modern military operations, challenging the boundaries of existing international legal frameworks. As nations incorporate increasingly advanced AI-driven systems with varying degrees of autonomy, the nature of traditional warfare is undergoing profound changes, prompting a reexamination of established legal principles and ethical standards. The emergence of AWS represents a paradigm shift in military technology, reshaping the dynamics of warfare. From their origins as remotely operated platforms, these systems have evolved into highly advanced entities, leveraging breakthroughs in artificial intelligence and machine learning to execute tasks with unparalleled precision and endurance. This evolution allows AWS to analyze vast amounts of data, make tactical decisions, and perform actions independently, transforming them from mere warfare tools to active participants in combat scenarios, capable of dynamically adapting to changing environments and opponent strategies. However, this progression also introduces significant ethical and legal dilemmas. Of particular concern is their ability to identify, select, and engage targets without direct human input- raising questions about distinguishing combatants and non-combatants, assessing proportionality, and ensuring ethically sound decisions in life-threatening scenarios[1].

The importance of clarifying the notion of 'Meaningful Human Control' is evident from the operational challenges and ethical risks highlighted by recent conflicts involving the deployment of autonomous systems in high-stakes environments. The wars in Nagorno-Karabakh[2] and Ukraine[3] have exposed critical gaps in control and accountability when autonomous systems are deployed without sufficient oversight. In these conflicts, AI-powered drones and autonomous weaponry were employed with varying levels of human involvement, which often resulted in operational ambiguities and raised serious ethical questions. These cases underscore the urgency of defining and operationalizing MHC in a way that can be effectively integrated into international regulations and military practices to prevent unintended escalatory conflicts, safeguard non-combatant safety, and ensure compliance with IHL. Beyond immediate military implications, the regulation of AWS and the application of MHC have far-reaching consequences for broader global security concerns, including arms races, ethical AI deployment,

[1] J. Van Den Boogaard (2016), *Proportionality and Autonomous Weapons Systems*.
[2] D. Hambling (2020), *The 'Magic Bullet' Drones Behind Azerbaijan's Victory Over Armenia*.
[3] J. Weber (2024), *Autonomous Drone Swarms and the Contested Imaginaries of Artificial Intelligence*.

and human rights protections. As the development of AWS accelerates, so too does the risk of an international arms race, with states competing to develop increasingly autonomous and potentially lethal technologies [4]. Without standardized regulations and widely accepted principles for MHC, this competition risks destabilizing international relations and escalating tensions among major powers. Furthermore, the ethical challenges posed by AWS extend beyond the battlefield, raising fundamental questions about the role of AI in life-and-death decisions and the protection of human dignity. The unchecked deployment of these technologies in conflict zones risks eroding ethical standards and violating IHL principles. Addressing these concerns requires a framework that prioritizes accountability, transparency, and effective human oversight to ensure that AWS align with international norms and moral values. Such a framework is essential to mitigate operational risks, uphold ethical standards, and maintain accountability in the face of escalating technological advancements.

Despite extensive discussions in high-profile international forums, such as the Convention on Certain Conventional Weapons (CCW), and insightful analyses by leading think tanks, including the Stockholm International Peace Research Institute (SIPRI) [5], a substantial consensus on defining and operationalizing MHC over AWS remains elusive. These deliberations, although robust, have not yet culminated in a universally accepted framework or set of standards, highlighting a significant gap in the international legal architecture. This absence of consensus is particularly problematic given the rapid pace at which AWS technologies are developing and being deployed in military contexts around the world. The current international discourse reveals a patchwork of national policies and guidelines that vary dramatically in scope and implementation, leading to a fragmented global approach that struggles to address the complexities introduced by autonomous military technologies effectively. As a result, there is an urgent need for an in-depth examination and clarification of MHC that can guide the international community toward unified regulatory standards and help bridge the divide between rapid technological advancement and existing legal infrastructures. These ethical and legal challenges underscore this imperative for robust human oversight in the operation of AWS. As highlighted by statements from the UN Secretary-General and the ICRC President[6], effective human control is crucial not only for ensuring that the development and actions of AWS are consistent with international norms and the principles of the laws of armed

[4] J. Dawes (2021), *UN Fails to Agree on 'Killer Robot' Ban as Nations Pour Billions Into Autonomous Weapons Research.*
[5] Ch. P. Trumbull (2019), *Autonomous Weapons: How Existing Law Can Regulate Future Weapons.*
[6] Chair's Summary (2024), *Humanity at the Crossroads: Autonomous Weapon Systems and the Challenge of Regulation*.

conflict but also for preserving accountability when violations occur. Maintaining such oversight ensures that decisions made by AWS align with ethical standards and are subject to human judgment and moral values, thereby preventing the dehumanization of warfare and reducing the risk of escalatory cycles that could result from autonomous actions.

This thesis endeavors to critically dissect the complex, yet pivotal concept of MHC within the regulatory scope of AWS. MHC is fundamental not only for aligning the operation of AWS with stringent ethical and legal standards but also for ensuring that such systems do not autonomously make decisions that could lead to unintended escalatory conflicts or violations of international law. However, the definition of MHC remains elusive and broadly interpreted across different national bodies and defense frameworks, resulting in significant governance voids. These gaps undermine efforts to establish a cohesive global stance on AWS regulation and pose serious challenges to maintaining international security and human dignity in warfare. The lack of a clear, universally accepted definition of MHC leads to inconsistencies in the application of AWS across various contexts and jurisdictions, intensifying the difficulties in formulating effective oversight and accountability measures.

As the capabilities of AWS advance, the international community faces pressing demands to reevaluate and strengthen the regulatory frameworks governing their use. This includes clarifying the definition and implementation of MHC, developing new norms and protocols that can adapt to technological growth, and ensuring that AWS are employed in a manner that upholds human dignity and promotes peace and security. Without agreed-upon standards, AWS may operate in ways that lead to unintended consequences, including potential violations of international law and infringements on human rights. Furthermore, this gap underscores the urgent need for a comprehensive global framework that can guide the deployment and use of AWS. Such a framework would need to harmonize the principles of human oversight, accountability, and transparency while ensuring that all state and non-state actors adhere to the same set of rules, thus maintaining international security and protecting human rights across all operational contexts. The development of this framework would also facilitate more straightforward guidelines for technologists and engineers in the design and implementation stages of AWS, ensuring that these systems are not only technologically advanced but also aligned with ethical standards and legal obligations. The pressing requirement for such a treaty

is underscored by international discussions, including those led by the ICRC and UN bodies[7], which emphasize the need for globally consistent regulatory standards and practices to manage the complexities introduced by AWS.

To address these pressing issues, this thesis transitions from identifying critical gaps in the regulation and oversight of AWS to proposing actionable frameworks that can guide the international community in establishing meaningful human oversight. By critically examining MHC as an evolving concept and analyzing key case studies, the research seeks to contribute valuable insights toward a framework that balances current technological advancements with long-standing legal and ethical principles. The ultimate goal is to provide a solid foundation that not only clarifies MHC but also offers practical pathways for integrating human control into AWS regulatory structures. In doing so, this thesis aims to foster greater accountability, adherence to international standards, and the preservation of human dignity as warfare technologies grow increasingly autonomous.

Methodology

To explore the complexities of AWS and the notion of 'Meaningful Human Control', this study adopts a multi-disciplinary methodological approach that integrates the analysis of key legal instruments and documents, military reports, and practical case studies. By leveraging a combination of primary and secondary sources, the research provides a holistic view of the current state and operational dynamics of AWS. The foundation of this analysis includes official documents from international negotiations and policy-making bodies, such as reports from the CCW meetings[8]. These documents are invaluable for understanding the evolving international consensus, as well as the debates and challenges involved in defining and implementing MHC in military technology. In addition to the primary sources, the study extensively uses academic literature and analyses from global defense studies to provide a broader context. Publications from think tanks like the SIPRI[9] and the International Institute for Strategic Studies (IISS)[10] offer insights into the strategic implications of AWS and the perspectives of various stakeholders in the defense community. These sources enrich the analysis by highlighting the

[7] N. Melzer (2017), *International Humanitarian Law – A Comprehensive Introduction.*
[8] UN (UNDOA), *Meetings of the Group of Governmental Experts* https://disarmament.unoda.org/meetings-of-the-group-of-governmental-experts/
[9] SIPRI, *Related publications: Autonomy in weapon systems,* https://www.sipri.org/research/armament-and-disarmament/emerging-military-and-security-technologies/autonomy-weapon-systems/recent-pubs
[10] IISS, *Our Publications, https://www.iiss.org/publications/*

ethical, legal, and practical considerations that influence AWS regulations. Practical examples of AWS deployment in conflict zones provide concrete data on how these systems are used in the field and the challenges they present. Recent conflicts, such as the Nagorno-Karabakh war, highlight the operational challenges of deploying drones and autonomous weapons, particularly in target identification, engagement protocols, and maintaining effective human oversight. These real-world scenarios are critical for understanding the gaps between theoretical frameworks and actual practice.

Overall, the thesis aims to bridge the significant gaps identified between current MHC practices and the ideal standards necessary to prevent unintended escalatory conflicts or violations of international law. By analyzing how MHC has been applied or overlooked in real-world scenarios, the study seeks to propose how international laws might evolve to better encompass the rapid advancements in military technology while ensuring that ethical and legal standards are maintained. By synthesizing these diverse sources, the research aims to offer actionable insights into how MHC can be more effectively integrated into military practice and regulatory frameworks. The ultimate goal is to contribute to the development of a robust, universally accepted definition of MHC that aligns with the rapid technological advances in AWS, promoting international security and the preservation of human dignity in warfare.

Research Question: Defining and Operationalizing 'Meaningful Human Control' in AWS Regulation

To guide the thesis, the primary research question poses a critical inquiry: *"How can the concept of 'Meaningful Human Control' be defined and operationalized in the regulation of Autonomous Weapon Systems to ensure compliance with International Humanitarian Law and accountability by parties to the conflict?"* This question serves as the central focus of the study, driving an examination that is essential not only for conceptual clarity but also for its real-world implications in military practice. Addressing these questions aims to bridge existing gaps in both theoretical understanding and the practical application of MHC, an area increasingly relevant as AWS technology advances and is adopted in varied global contexts.

The research question situates MHC at the intersection of legal standards and operational integrity in warfare, underlining its necessity in aligning AWS deployment with the principles of IHL. The aim here is not solely to propose a theoretical definition of MHC but to identify

and detail how it can be effectively integrated into military practice to guide decision-making, maintain human oversight, and ensure compliance with established norms and protocols of warfare. By operationalizing MHC, the study seeks to provide a foundation for implementing control mechanisms that would prevent autonomous systems from engaging in unregulated or unintended escalatory conflicts [11], where human oversight might otherwise be absent. Furthermore, the question underscores the scope of MHC's applicability, emphasizing that it extends beyond legal compliance to encompass the preservation of ethical norms and accountability in conflict. This inquiry paves the way for an in-depth analysis of MHC's role in safeguarding against potential breaches of international standards, aiming to establish MHC as an essential element of AWS governance that maintains accountability, even amid rapid technological advancement. This research question also directly engages with global concerns surrounding AWS, especially the challenge of maintaining human oversight within increasingly autonomous warfare systems, a challenge extensively discussed by Paul Scharre [12] in his analysis on the operational risks of autonomous weapons. These concerns are not limited to national or military interests, they implicate broader international security, accountability, and humanitarian protections. By exploring MHC's application, the question highlights the urgent need for global governance structures that can consistently manage AWS across jurisdictions, ensuring systems are used responsibly and with due regard for human rights and international stability. The study's examination of MHC within AWS frameworks contributes to this broader conversation, providing a framework that not only informs military applications but also offers insights valuable to international policymakers, human rights advocates, and regulatory bodies. As the global community continues to confront the ethical and legal implications of AWS, the operationalization of MHC may prove essential for mitigating risks associated with unregulated autonomy in warfare.

To fully address the primary research question on defining and operationalizing MHC in AWS, the thesis delves into a series of critical sub-questions. These sub-questions serve as a structured framework to unpack the key ethical, legal, and operational considerations surrounding MHC and to establish a roadmap for developing a comprehensive regulatory framework.

- The first sub-question examines how current international laws and treaties, including the Geneva Conventions and their Additional Protocols, as well as AWS-specific

[11] F. Sauer (2021), *Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible.*
[12] P. Scharre (2016), *Autonomous Weapons and Operational Risk.* Center for a New American Security.

discussions under the United Nations, address (or fail to address) the requirements for human oversight in autonomous systems (Chapter 1). Although these legal frameworks provide foundational principles, they often lack explicit provisions for AWS, particularly concerning the degree of human control required. Here, the study will analyze how MHC can bridge these legal gaps by offering a standardized approach to AWS oversight that aligns with existing laws but also adapts to the unique capabilities and risks associated with autonomy. This section will evaluate how MHC could function as a stabilizing factor within international law, ensuring that AWS adhere to established norms and that human agents remain accountable for critical decisions. By pinpointing the deficiencies in current international instruments, the thesis will highlight the need for MHC as an adaptive mechanism that ensures AWS operate within legal constraints and avoid unlawful actions or unintended escalations.

- The second sub-question explores the core challenges that AWS introduce across ethical, legal, and operational domains (Chapter 2). This section will explore how MHC functions as a necessary safeguard to uphold these considerations. Ethical challenges involve safeguarding non-combatants and upholding principles of proportionality, which are designed to minimize harm to civilians and infrastructure. By examining these ethical requirements, the study will assess the role of MHC in preventing AWS from engaging in actions that may breach these foundational principles. Legal challenges will focus on the requirements established by IHL, such as the principles of distinction, proportionality, and necessity[13], which dictate the limits of force in armed conflicts. MHC plays a pivotal role in aligning AWS with these legal standards by ensuring that human agents oversee and validate actions that have potentially lethal consequences. Operational challenges will address the technical reliability and decision-making capabilities of AWS, emphasizing the importance of MHC in maintaining control over systems that must operate effectively under unpredictable conditions. Together, these ethical, legal, and operational factors form the foundation for understanding why MHC is essential for AWS and for identifying the constraints and conditions under which AWS may be permitted in military contexts.

[13] Ch. P. Trumbull (2019), *Autonomous Weapons: How Existing Law Can Regulate Future Weapons.*

- The third sub-question focuses on the role of MHC in establishing accountability within AWS operations, particularly in maintaining a transparent chain of responsibility (Chapter 3). MHC serves as a critical mechanism for ensuring that all actions undertaken by AWS can be traced back to human agents, reinforcing the principle that responsibility for AWS actions ultimately resides with humans. This aspect of MHC addresses both military accountabilities[14], where command structures necessitate clear chains of responsibility, and public accountability[15], which demands transparency in the deployment and consequences of AWS actions. By examining procedural mechanisms that enforce MHC, such as authorization protocols and operational oversight requirements, this section will highlight the operational safeguards necessary to ensure that AWS actions are consistent with international accountability standards. The analysis will emphasize the practical ways in which MHC can prevent the delegation of decision-making authority to autonomous systems, particularly in situations where life-or-death outcomes are involved. Ensuring that MHC remains central to AWS operations thus becomes essential for preserving human accountability and reinforcing the ethical standards expected in military conduct.

- The fourth and final sub-question examines the fundamental components required to establish a legal framework capable of effectively regulating AWS and maintaining MHC (Conclusion). This framework will need to prioritize transparency, accountability, and technical standards to ensure AWS operations remain traceable and governed by clear, enforceable guidelines. Transparency requires that AWS actions are documented and auditable, allowing for post-operation review and accountability. Accountability would be maintained through procedural protocols that assign responsibility to human agents, ensuring that AWS decisions are traceable and that any breaches can be attributed to accountable parties. In terms of technical standards, this framework must incorporate specifications that limit AWS autonomy to defined boundaries, enforcing MHC in all operational stages. Moreover, the framework should emphasize future-proofing provisions, recognizing the rapid pace of technological advancement in AWS capabilities. By proposing adaptable legal standards, this chapter will explore how MHC can remain effective over time, ensuring that any legal framework developed for AWS

[14] CCW GGE on LAWS (2024), *Measures needed to ensure compliance with IHL and the identification of potential additional measures.*
[15] J. Kwik (2022), *A Practicable Operationalization of Meaningful Human Control.*

regulation remains relevant and resilient in light of ongoing advancements in AI and military technology.

Chapter 1. Frameworks of Control: Defining the Intersection of IHL Principles and AWS

The rapid integration of AWS into modern military operations marks a pivotal evolution in warfare, presenting unprecedented challenges for existing international legal frameworks, which are currently ill-equipped to manage these advanced technological scenarios effectively. These systems, operating with varying degrees of autonomy, not only push the ethical and legal boundaries within the established framework of IHL but also necessitate a reevaluation of foundational principles such as proportionality, distinction, and military necessity[16]. The recent deployments in the Nagorno-Karabakh conflict and the ongoing situation in Ukraine starkly illustrate the deficiencies of current regulatory frameworks, which struggle to keep pace with AWS's rapid development and operational independence. Specifically, in these conflicts, autonomous drones were deployed with minimal human oversight, leading to increased civilian casualties and unintended military engagements. These instances vividly showcase how the lack of stringent control mechanisms can lead to significant violations of the core principles of IHL. This underscores the critical need for enhanced regulatory measures that integrate MHC to ensure that decision-making in the deployment of AWS adheres to legal and ethical standards, thereby preventing such detrimental outcomes[17].

The concept of 'Meaningful Human Control' plays a pivotal role in addressing the significant challenges posed by AWS. By integrating human judgment into AWS decision-making processes, MHC ensures that operations adhere to the legal principles mandated by IHL. MHC is essential for addressing the deficiencies within current legal frameworks that fail to adequately oversee autonomous weapon systems. By ensuring that critical decision-making remains under human supervision, MHC not only aligns the deployment of AWS with the core principles of IHL but also enhances accountability and transparency. This approach is crucial as AWS increasingly undertake roles that could result in decisions with potentially lethal outcomes, raising pressing questions about accountability and compliance with established international standards.

[16] N. Melzer (2017), *International Humanitarian Law – A Comprehensive Introduction.*
[17] J. Kwik (2022), *A Practicable Operationalization of Meaningful Human Control*.

Central to this chapter is the critical inquiry: *"How do existing international laws address or fail to address the need for human oversight in AWS?"* This pivotal question guides our exploration and analysis. By examining the IHL principles of proportionality, distinction, and military necessity, the analysis reveals significant gaps within current legal frameworks and explores how MHC could serve as a vital mechanism to address these deficiencies. This critical examination lays the groundwork for a comprehensive understanding of MHC's role in enhancing AWS regulation and aligning them with international legal standards.

As the chapter unfolds, it defines and contextualizes key IHL principles within the scope of AWS regulation, evaluates the effectiveness of existing legal frameworks, such as the Geneva Conventions and the CCW, and identifies where they fall short in addressing the unique challenges posed by AWS. A focused gap analysis further underscores the importance of MHC, positioning it as an essential element in reforming AWS oversight. By pinpointing these deficiencies, the chapter prepares the groundwork for in-depth discussions on operationalizing MHC to achieve ethical and lawful AWS regulation.

1.1. Autonomous Weapon Systems and IHL: Core Principles and Modern Challenges

The objective of this section is to meticulously define and elucidate the foundational principles of IHL that are pivotal to the regulation of AWS. This exploration is crucial for understanding how AWS, with their advanced autonomous capabilities, fundamentally challenge and stretch the traditional boundaries of IHL. By defining these principles – distinction, proportionality, and military necessity – the goal is to critically analyze the implications of AWS deployment in modern warfare, highlighting the legal and ethical modifications necessary to accommodate these technological advancements. This detailed analysis will provide a foundation for exploring how these principles can be adapted or reinterpreted to remain relevant and practical in light of advancing military technologies.

The principle of distinction represents a cornerstone of IHL that is fundamental to lawful warfare. This principle, as codified in Article 48 of AP I to the Geneva Conventions[18], requires combatants to differentiate at all times between military targets and civilians, a task that becomes exceedingly complex with the deployment of AWS. For the principle of distinction, the integration of sophisticated sensor technologies is paramount. Multimodal sensors, which

[18] ICRC, *Article 48 – Basic rule.*

combine visual, infrared, and radar data, can enhance an AWS's ability to distinguish between combatants and civilians in complex environments. Machine learning techniques, such as pattern recognition and neural systems, minimize the risk of misclassification in densely populated areas. These systems must be meticulously programmed to navigate the nuanced environments of the battlefield, where the ability to distinguish accurately is crucial.

AWS, equipped with advanced sensing and targeting capabilities, theoretically have the potential to enhance adherence to this principle. Yet, the practical application is fraught with challenges due to the complexity of battlefield scenarios. Current AWS technologies may struggle with the precise identification of targets in situations where combatants and civilians are closely intermingled, leading to potential misidentifications and unintended casualties. Specific challenges include distinguishing between combatants who are wounded or surrendering – a process that can vary significantly across different cultures, and civilians actively participating in hostilities. Additionally, some objects serve both civilian and military purposes, known as dual-use items. Ethical debates surrounding the principle of distinction often highlight the severe consequences of misidentification, which can lead to significant legal repercussions under international law. For instance, historical precedents such as the erroneous targeting incidents during the conflicts in Iraq and Afghanistan – such as the 'Haditha killings'[19] and the 'Kill or Capture'[20] operations – have been scrutinized in international courts. These cases highlight the crucial importance of adhering strictly to the principle of distinction and underscore the legal and moral obligations to enhance AWS capabilities. Ensuring that their programming is sophisticated enough to prevent such errors and align with the strict standards of IHL is essential. Jeroen van den Boogaard's[21] insights highlight the importance of refining AWS programming to manage these distinctions better. Improving these systems involves not only advancing the technological capabilities of AWS but also ensuring that they are embedded with an in-depth understanding of the contextual battlefield dynamics. Crucially, this improvement must be complemented by consistent human oversight, where decision-makers interpret the data provided by AWS to ensure decisions are ethically and legally sound. This is essential to prevent the misidentification of civilians as combatants, a serious breach of IHL.

[19] In 2005, during the Iraq War, U.S. Marines killed 24 Iraqi civilians, including women and children, in response to a roadside bomb attack. This incident underscored the challenges of adhering to the principle of distinction, as civilians were mistakenly identified as combatants in the chaotic war environment, leading to court-martial proceedings.

[20] Operations, particularly prominent during the Afghanistan War (2001–2021), targeted suspected militants but often led to civilian casualties due to intelligence errors, breaching the principle of distinction under IHL. These operations faced criticism in human rights and legal forums for failing to protect non-combatants.

[21] J. Van Den Boogaard (2016), *Proportionality and Autonomous Weapons Systems*.

To effectively meet these challenges, it is imperative to enhance AWS decision-making algorithms to distinguish between combatants and civilians more reliably. This process should be supported by comprehensive testing and validation across varied operational settings and continuously monitored by human oversight to ensure decisions align with ethical and legal standards. Ultimately, achieving this level of distinction requires international cooperation to standardize the deployment of AWS in warfare, ensuring they operate within the structures of IHL and uphold the integrity of military engagements.

Having examined how AWS must be meticulously programmed to uphold the principle of distinction, ensuring that combatants are always differentiated from civilians, it is imperative to shift our focus to another crucial aspect of lawful engagement under IHL: proportionality. This principle, as codified in Article 51(5)(b) of AP I to the Geneva Convention[22], requires that any collateral damage to civilians or civilian property must not be excessive in relation to the concrete and direct military advantage expected from a military operation. AWS, with their capabilities for independent action, pose unique challenges in adhering to this principle due to their ability to execute decisions rapidly and on a scale beyond human operators.

According to Vincent Boulanin et al.[23], AWS require programming that can precisely assess military advantages and potential collateral impacts in real-time, ensuring that their operations strictly comply with the principle of proportionality. This necessitates the development of AI-driven risk assessment algorithms that play a critical role in calculating the expected military advantage of an attack and weighing it against potential civil harm. Advanced machine learning models are increasingly being utilized to refine these assessments, enabling real-time updates as battlefield conditions change. Such advancements are critical to enhancing the precision of AWS in complex combat environments, addressing both ethical concerns and operational requirements. However, despite these technological advancements, the final assessment of proportionality must be conducted by a human, who evaluates the data provided by the AI to ensure that decisions align with ethical and legal standards. The rapid execution capabilities of AWS highlight the need to update the international legal framework, which should encompass provisions for real-time proportionality assessments. Modifications to international treaties are crucial, as they must explicitly govern the deployment of AWS by integrating clauses that mandate compliance with dynamic proportionality evaluation during military operations. Such

[22] ICRC, *Article 51- Protection of the civilian population.*
[23] V. Boulanin et al. (2021), *Autonomous Weapon Systems and IHL*.

legal updates would provide a clear legal basis for the use of AWS, ensuring their actions remain consistent with international humanitarian standards while leveraging their technological capabilities to minimize unintended harm. As underscored by the Stockholm International Peace and Research Institute (SIPRI)[24], integrating these algorithmic safeguards is essential not only for technological advancement but also for ensuring that AWS operations remain within the boundaries set by international law. SIPRI advocates for global cooperation to establish norms that prevent AWS from exceeding the proportional responses traditionally expected in warfare, thereby supporting their ethical integration into military operations.

Building on the discussion of proportionality, the principle of military necessity represents another cornerstone of IHL that is fundamental to lawful warfare. Under the principle of military necessity, decision-making algorithms play a crucial role in determining the minimum necessary force required to achieve a specified military objective. These algorithms analyze various factors, including the type of target, the surrounding environment, and potential collateral damage. By incorporating scenario simulation technologies, AWS can predict the outcomes of different actions, helping to ensure that the use of force is both measured and legally justified. This principle refines the use of military force by demanding that actions are confined strictly to legitimate objectives, thus adding another layer of complexity for AWS in terms of operational ethics and legal compliance.

Military necessity dictates that the application of force in military operations must be confined strictly to legitimate military objectives, which are crucial for achieving a definitive military advantage. This principle challenges AWS, which, rather than operating autonomously, must incorporate human oversight to determine the necessity and proportionality of force without causing undue harm or suffering. This human oversight requirement reflects the directives from the UN[25] and the ICRC[26], which both call for a ban on fully autonomous systems that operate without human control. The unique capability of AWS to independently analyze and engage targets necessitates algorithms that are not only precise but also inherently capable of rapid assessment and response according to the fluid dynamics of combat situations. The complexity of AWS operations necessitates that these systems are equipped with decision-making algorithms capable of distinguishing between legitimate military targets and non-combatants.

[24] V. Boulanin et al. (2020), *Autonomy in Weapon Identifying Practical Human Control*.
[25] CCW (2019), *Guiding Principles Affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems.*
[26] ICRC (2022), *ICRC Position on Autonomous Weapon Systems*.

This entails a sophisticated understanding of the context and the ability to adjust actions in real-time to mitigate the risks of unlawful engagements. The legal and ethical deployment of AWS depends on their ability to consistently apply these criteria under the rigorous standards of military necessity, ensuring operations strictly target military objectives and avoid actions that could lead to unnecessary or unlawful harm. The application of military necessity within the realm of AWS demands substantial policy adaptation to ensure legal compliance. Revisions to rules of engagement are imperative to encapsulate the capabilities and limitations of these autonomous systems, proposing a framework that facilitates their ethical integration into military operations. An international agreement outlining strict guidelines for AWS deployment could standardize how these systems evaluate military objectives, ensuring their actions are both legally justified and ethically sound. Such policy reforms would not only address the rapid advancements in autonomous technology but also strengthen the global governance of military engagements to uphold the rigorous standards of military necessity. The focus should remain on refining these technologies under human oversight to meet the stringent demands of military necessity, fostering a balance between technological innovation and adherence to international law. This ensures that while AWS capabilities advance, they do not autonomously make critical decisions without human judgment guiding and validating these actions.

1.2. Assessing AWS Human Oversight through Legal and Academic Perspectives

This comprehensive section bridges the gap between the practical implications within existing legal frameworks and scholarly discussions on human oversight in AWS. By integrating these two perspectives, the analysis not only highlights the theoretical debates surrounding 'Meaningful Human Control' – a critical concept in ensuring that AWS operations align with human ethical standards – but also scrutinizes how these discussions are reflected and addressed within international legal standards. This dual approach offers a comprehensive view of the current state of AWS regulation, highlighting both the depth of academic discourse and the concrete legal challenges presented by the deployment of autonomous technologies in military contexts.

To begin, it's crucial to focus on a detailed examination of the legal frameworks that govern the deployment and operation of AWS. This part of our analysis critically evaluates how international laws, including various conventions and protocols, navigate the operational and ethical complexities introduced by AWS. Emphasizing the compatibility of these legal

standards with the principles of MHC, examining their efficacy in keeping pace with the rapid advancements in military technologies.

The 1977 Additional Protocols to the Geneva Conventions, specifically Articles 36 and 92[27], establish the framework for legal reviews of new weapons systems, including AWS. Article 36 requires that any new weapon, means, or method of warfare undergo a thorough legal review that confirms its compatibility with international law. This process is vital to ensure that AWS, which can make autonomous decisions in battlefield scenarios, operate within the constraints of international humanitarian standards. The legal reviews focus on the system's ability to adhere to principles such as distinction and proportionality, which are central to maintaining MHC in military operations. However, a significant gap in the application of these articles arises from their lack of explicit guidance on how these principles should adapt to the unique challenges posed by AWS. This oversight in the legal framework can lead to inconsistencies in the operationalization of MHC, as current guidelines may not fully address the advanced decision-making capabilities and potential for autonomous action inherent in AWS. Addressing these gaps is essential to ensuring that AWS operations are conducted under stringent ethical and legal oversight, reinforcing their alignment with both the spirit and the letter of IHL.

Moving from broad provisions of IHL to the more specific mandates of the Geneva Conventions, we encounter a foundational aspect of IHL that directly impacts AWS operations. The Geneva Conventions, enhanced by their Additional Protocols, set the cornerstone of international legal standards for the conduct of war, with a strong emphasis on protecting civilians and adhering to the principle of distinction. These legal standards are crucial for ensuring that AWS can effectively distinguish between combatants and non-combatants, a fundamental requirement to uphold MHC (Geneva Conventions, AP I, Art 48[28]; ICRC, Rules 1 and 7[29]). Yet, the autonomous capabilities of AWS introduce significant complexities in maintaining consistent compliance with these norms. The challenge of programming AWS to replicate nuanced human decision-making reveals substantial accountability gaps. Specifically, when AWS operate without effective human oversight, the accountability for decisions made by these systems becomes ambiguous. This lack of clear accountability is problematic because, unlike humans, machines cannot be held responsible for their actions. This gap highlights the crucial need for

[27] ICRC, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.*
[28] ICRC, *Article 48 – Basic rule.*
[29] ICRC, *Rules,* IHL DATABASES, https://ihl-databases.icrc.org/en/customary-ihl/v1

robust legal and operational frameworks that not only enforce but also clarify the accountability of AWS, ensuring that these systems are not operating in a vacuum of responsibility and that their actions are consistently aligned with human ethical and legal standards. This demands a robust definition of MHC.

As we consider the legal implications of AWS under the Geneva Conventions, it is also crucial to examine broader legal principles, such as those encapsulated in the Martens Clause and human rights law, which offer additional layers of protection and ethical guidance. The Martens Clause[30] reinforces existing legal norms by asserting that in the absence of explicit legal regulations, the conduct of hostilities remains governed by the principles of humanity and the dictates of public conscience. This clause is particularly relevant in discussions on AWS, which may operate in contexts not yet explicitly regulated by international agreements. Advocacy groups, such as Human Rights Watch[31], emphasize the importance of aligning AWS operations with these broad principles to ensure that actions taken by autonomous systems adhere to human moral values. The inclusion of the Martens Clause in AWS regulations serves as an ethical guide in modern warfare, ensuring that the deployment and use of these technologies respect humanity and public conscience. It requires the international community to consider how AWS can comply with broader human rights obligations, thus reinforcing the role of MHC in bridging the gap between rapid technological advancements and the slower pace of legislative responses. Implementing guidelines that respect the Martens Clause can help ensure that AWS operations are not only technologically advanced but also ethically grounded, promoting a balance that aligns with international human rights standards.

With the foundational principles and broader legal doctrines discussed, the focus now shifts to specific international frameworks that address contemporary weapons technologies, particularly the CCW. The CCW framework[32] has become an essential arena for global discussions about the deployment and regulation of AWS, focusing on their compatibility with established norms of ethical warfare and IHL. These discussions critically assess whether the existing legal instruments within the CCW sufficiently govern AWS or if new protocols are needed that are tailored specifically to the nuances of these systems. In these deliberations, AWS-specific discussions under the CCW framework have highlighted the impact of autonomous technologies on contemporary warfare practices and the challenges they pose to

[30] ICRC, *Martens Clause "How Does Law Protect in War?*
[31] V. Boulanin et al. (2021), *Autonomous Weapon Systems and IHL*.
[32] CCW GGE on LAWS (2024), *Existing IHL applicable on LAWS.*

upholding international ethical standards. Notably, Article 36 of AP I to the Geneva Conventions requires states to conduct legal reviews of new weapons, means, or methods of warfare, making it particularly relevant in assessing whether AWS can comply with fundamental IHL principles. Additionally, Articles 51 and 57 of AP I outline obligations related to distinction, proportionality, and precaution in attack, which are core principles that AWS must adhere to in military operations. These articles are frequently referenced in CCW debates as benchmarks for assessing the legality of autonomous targeting and decision-making. The discourse within the CCW has increasingly emphasized the need for protocols that ensure AWS operations are conducted under meaningful human oversight. This alignment is crucial for integrating MHC into the legal framework, thereby reinforcing the integrity of military conduct and ensuring that AWS operations adhere strictly to principles of humanity and accountability. Such a focus underscores the urgency of developing comprehensive guidelines that not only address the operational capabilities of AWS but also their ethical implications, ensuring that all deployments are consistent with the high standards expected in international law.

Despite extensive discussions within existing legal frameworks regarding AWS, substantial gaps remain, particularly in defining and implementing MHC. These deficiencies are highlighted by scholars such as Anna-Katharina Ferl[33], who points to a persistent ambiguity surrounding MHC in international discussions. Ferl's analysis highlights the absence of a standardized definition, which complicates the consistency and applicability of MHC in AWS operations across various jurisdictions. Furthermore, the challenges of integrating MHC into the lifecycle of AWS, as examined by Lena Trabucco[34], reveal significant issues with accountability mechanisms. Trabucco emphasizes that without a clear operational definition of MHC, determining accountability in the deployment of autonomous systems becomes fraught with legal complexities. Recent conflicts and international debates provide concrete examples of these gaps in action. For instance, discussions within the framework of the CCW have repeatedly highlighted the difficulty in reaching a consensus on what constitutes MHC[35]. These debates reflect the international community's struggle to align rapidly advancing military technologies with existing ethical and legal standards. Moreover, the deployment of AWS in conflict zones, such as Nagorno-Karabakh, has exposed the practical implications of these

[33] A.-K. Ferl (2023), *Imagining Meaningful Human Control: Autonomous Weapons and the (De-)Legitimisation of Future Warfare.*
[34] L. Trabucco (2023)*, What Is Meaningful Human Control, Anyway? Cracking the Code on Autonomous Weapons and Human Judgment*.
[35] J. Kwik (2022), *A Practicable Operationalization of Meaningful Human Control*.

regulatory gaps. The use of autonomous drones (Turkish-made Bayraktar TB2 drones)[36] in this region has led to incidents where the lack of adequate human oversight resulted in breaches of the principles of distinction and proportionality, thus demonstrating the urgent need for explicit regulatory guidelines that define and enforce MHC. These examples not only illustrate existing deficiencies but also underscore the need for enhanced regulations that are explicitly tailored to AWS. There is a pressing need for a clear, actionable framework that expressly outlines the parameters of MHC, ensuring that AWS operations adhere to both the spirit and the letter of international law. This would involve establishing a universally accepted definition of MHC that can guide the development, deployment, and use of AWS, ensuring that they operate within the bounds of ethical warfare and remain consistently accountable to human judgment and oversight.

Transitioning from the legal perspectives, our analysis now shifts to a detailed examination of the scholarly discussion on human oversight that governs the deployment and operation of AWS. To begin, it's crucial to synthesize the substantial scholarly contributions that delve into human oversight in AWS, with a particular emphasis on the concept of MHC. The International Committee of the Red Cross (ICRC) and the Stockholm International Peace Research Institute (SIPRI) are notable organizations that advocate for the integration of human judgment in the deployment of these systems. The ICRC[37] has consistently emphasized that MHC is crucial for ensuring that AWS operations adhere to the principles of IHL, particularly regarding the protection of civilian populations in conflict zones. Their reports and position papers emphasize that without significant human oversight, AWS may fail to distinguish adequately between combatants and non-combatants, thereby raising significant ethical and legal concerns. Similarly, SIPRI's[38] research highlights the technical and ethical challenges posed by AWS. Their studies suggest that while AWS can enhance operational efficiency, their use also raises profound questions about the moral implications of delegating critical combat decisions to machines. SIPRI advocates for stringent standards that ensure robust human control mechanisms govern AWS operations, maintaining accountability and preventing unintended escalations in hostilities. Together, these organizations contribute to a growing body of literature that seeks to define the boundaries and expectations for MHC within AWS deployments. They argue that effective human oversight is not only a regulatory requirement

[36] D. Hambling (2020), *The 'Magic Bullet' Drones Behind Azerbaijan's Victory Over Armenia*.
[37] ICRC (2022), *ICRC Position on Autonomous Weapon Systems*.
[38] V. Boulanin et al. (2020), *Autonomy in Weapon Identifying Practical Human Control.*

but a fundamental aspect of maintaining the ethical integrity of military engagements under the framework of IHL.

The scholarly landscape surrounding MHC in AWS is marked by vigorous debate and a spectrum of viewpoints, each emphasizing the critical balance between technological autonomy and human ethical oversight necessary to navigate the complexities of modern warfare.

A primary concern among scholars like Anna-Katharina Ferl[39] is the essential role of MHC in preserving human dignity and ensuring accountability within automated military operations. She emphasizes that without direct human involvement, AWS decisions might lack the necessary ethical and contextual judgment to uphold the principles of humane warfare. Expanding on this, Vincent Boulanin and his colleagues[40] address the challenges posed by the rapid technological advancements in autonomous systems and the slower pace of evolution in legal frameworks. Their analysis delves into how emerging technologies can be harmonized with the rigid structures of IHL, highlighting the significant challenges in ensuring that AWS deployments are both legally compliant and ethically sound. Scholars like Paul Scharre[41] elaborate on the operational intricacies of AWS, highlighting the technical and ethical hurdles in implementing effective human oversight. He advocates for transparent algorithms and a human-in-the-loop approach as fundamental to any AWS deployment strategy that seeks to uphold MHC, ensuring that ethical considerations remain at the forefront of military engagements. Furthering this discussion, Jeroen van den Boogaard[42] delves into the dilemmas posed by the inherent characteristics of AWS, such as their capacity for rapid information processing and decision-making. He illustrates how these capabilities might undermine AWS's ability to adequately assess attack proportionality, thereby raising the risk of excessive collateral damage, a critical concern for MHC. Adding a philosophical perspective, Peter Asaro[43] discusses the broader ethical implications and the potential for dehumanization inherent in AWS. He calls for stringent regulations and a comprehensive ethical framework to govern the deployment of AWS, calling for an international ban on lethal autonomous weapons to reinforce the global commitment to MHC. In a similar vein, Daniele Amoroso and Guglielmo

[39] A.-K. Ferl (2023), *Imagining Meaningful Human Control: Autonomous Weapons and the (De-)Legitimisation of Future Warfare.*
[40] V. Boulanin et al. (2021), *Autonomous Weapon Systems and IHL*.
[41] P. Scharre (2016), *Autonomous Weapons and Operational Risk*, Center for a New American Security.
[42] J. Van Den Boogaard (2016), *Proportionality and Autonomous Weapons Systems*.
[43] P. Asaro (2012), *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-making.*

Tamburrini[44] provide a detailed exploration of how MHC can be operationalized within AWS frameworks. They propose a normative model that stresses the ethical responsibilities of developers and operators, ensuring that AWS operations remain under MHC to prevent unethical outcomes. Their comprehensive analysis highlights the potential of MHC to bridge the gap between technological capabilities and the ethical imperatives dictated by IHL.

Together, these scholarly discussions underscore the complex interplay between technology, law, and ethics in the realm of military automation, highlighting the urgent need for a cohesive framework that can effectively integrate MHC, thereby anchoring AWS within the bounds of international law and human moral principles. However, current academic frameworks often fall short in effectively addressing the rapid advancement and unique capabilities of AWS. These scholarly discussions reveal significant gaps in ensuring adequate human oversight, which many scholars argue could be mitigated through enhanced legal measures and robust technical safeguards. In this vein, Henrik Syse[45] underscores the importance of crafting explicit legal and operational definitions of MHC. He argues that a universally accepted delineation of MHC is crucial for its consistent application across diverse military operations and legal regimes. Syse advocates for detailed guidelines that clarify the roles and responsibilities of human operators within AWS frameworks, ensuring that ethical considerations are integral to every aspect of military engagement. This call for precise definitions is echoed across the literature, where a broad consensus supports the need for an international standard that explicitly outlines the parameters of human involvement in the deployment and operation of AWS.

1.3. Concluding Remarks

The exploration of international legal frameworks and the scholarly discussions surrounding the deployment of AWS highlight significant regulatory gaps and the urgent need for a comprehensive oversight mechanism. The principle of MHC emerges as a pivotal solution to these challenges, bridging the gap between the rapid advancements in military technologies and the slower evolution of legal standards. This analysis has delineated the gaps within existing frameworks – particularly in ensuring that AWS operations conform to the principles of distinction, proportionality, and military necessity as outlined by IHL. Looking ahead, the

[44] D. Amoroso and G. Tamburrini (2021), *Toward a Normative Model of Meaningful Human Control Over Weapons Systems*.
[45] H. Syse (2023), *Meaningful Human Control*.

insights gained from this critical examination lay a robust foundation for the subsequent chapter, which will delve into the operational and practical implementations of MHC. The forthcoming discussions aim to translate the theoretical frameworks of MHC into actionable guidelines and protocols that ensure AWS are deployed in a manner that is both ethically sound and legally compliant. Reiterating the importance of MHC, it is clear that defining this concept within legal contexts is essential for the lawful regulation of AWS. A universally accepted definition would not only enhance accountability but also ensure that AWS operations are consistently aligned with human ethical standards across various military and legal landscapes. Thus, this chapter sets the stage for developing comprehensive strategies that integrate MHC effectively, ensuring that AWS contribute positively to modern warfare without compromising ethical and legal norms.

Chapter 2. Human Oversight in Autonomous Warfare: Ethical, Legal, and Operational Imperatives

As the integration of AWS increasingly influences the dynamics of modern warfare, it becomes imperative to address the complex ethical and operational challenges posed by these technologies. This chapter focuses on how MHC is crucial for aligning AWS operations with international legal standards and ethical principles of warfare. It emphasizes the need for a balanced approach where technological autonomy is complemented by rigorous human oversight to ensure ethical conduct in military operations. The deployment of AWS raises complex questions about maintaining human dignity and adhering to established warfare norms, such as the protection of civilian lives and infrastructure. These systems' ability to make autonomous decisions challenges conventional warfare and accountability frameworks, potentially leading to actions that contravene principles such as proportionality and distinction, unless effectively moderated by human intervention.

Navigating through intersections of technology, policy, and human values, illuminating pathways towards a governance model that effectively manages the dynamics introduced by AWS. This chapter will examine the primary ethical and operational challenges in maintaining MHC, highlighting the crucial role of MHC in ensuring that AWS operations comply with both the spirit and the letter of IHL. By examining the roles of stakeholders, from developers and military strategies to international regulatory bodies, this analysis highlights the evolving expectations and responsibilities necessary for the ethical integration of AWS into military

operations. Insights from key organizations, such as the International Committee of the Red Cross (ICRC) and the Stockholm International Peace Research Institute (SIPRI), which lead the discourse on AWS and ethical frameworks, will provide essential perspectives on the current and future landscapes of warfare.

As this chapter progresses, it systematically addresses the ethical, legal, and operational challenges posed by AWS. It begins by assessing the moral implications of autonomous decisions and their real-world impacts, with a particular focus on the role MHC plays in safeguarding civilian life during conflict. The chapter then analyzes the legal responsibilities of developers, military strategists, and international bodies, emphasizing how their roles converge to reinforce MHC within AWS operations. Following this, it explores the operational challenges, evaluating the technical reliability and decision-making capabilities of AWS, and how MHC serves as a crucial control mechanism in various operational contexts. Each section builds upon the insights from the last, elaborating how MHC can bridge the gap between technological advancements and enduring ethical standards, ensuring AWS operate within the frameworks of international law and human values.

This integrated approach not only addresses the sub-question *"What are the key ethical, legal, and operational challenges in maintaining meaningful human control over AWS?"* but also sets the stage for a comprehensive discussion on how MHC functions as a pivotal element in bridging the gap between rapid technological advancements and enduring human values.

2.1. Safeguarding Humanity: The Crucial Role of Human Oversight in AWS

The deployment of AWS in modern warfare presents significant ethical challenges, especially regarding the protection of civilian lives and adherence to rigorous principles of warfare ethics. Central to addressing these challenges is the implementation of MHC, which ensures that AWS operations comply with the ethical standards mandated by IHL. MHC introduces a critical layer of human judgment and accountability in the deployment of AWS, crucial for upholding the principles of distinction and proportionality – key tenets of IHL that aim to protect civilian populations and ensure that the use of force is necessary and measured. Critics like Peter Asaro[46] argue that delegating lethal force to autonomous systems without robust human

[46] P. Asaro (2012), *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-making.*

oversight could violate fundamental human rights, such as the right to life and the principles of judicial due process. The lack of capacity for moral reasoning and contextual understanding in AWS raises concerns about their ability to make judicious decisions in complex, fluid combat environments. Without MHC, AWS risk carrying out lethal operations that inadequately distinguish between combatants and non-combatants, resulting in disproportionate civilian casualties and breaches of international law. Moreover, the fundamental ethical issue is whether machines should be allowed to make ultimate life-and-death decisions, a question that strikes at the core of human moral values and ethical conduct of warfare. The Campaign to Stop Killer Robots [47] strongly advocates for banning fully autonomous weapons, emphasizing that eliminating human oversight in decisions involving lethal force represents a significant moral and ethical violation. The campaign underscores the dehumanizing nature of AWS, warning that the absence of MHC could reduce life-and-death decisions to a detached, algorithmic process devoid of human accountability and empathy. Their campaign underscores the necessity of maintaining human involvement in military operations involving lethal force, not just for legal compliance but for preserving human dignity and ethical integrity in warfare[48]. Incorporating MHC into AWS operations is thus essential for maintaining ethical compliance and safeguarding civilian lives. It ensures that every deployment of lethal autonomous technology is evaluated and controlled by human agents, aligning technological advancements with enduring moral and ethical values.

Building on the foundational principles outlined previously, the real-world implications of AWS in conflict zones, such as Ukraine and Nagorno-Karabakh, starkly illustrate the ethical breaches that can occur without MHC. In Ukraine, AI-driven drones[49] have been reported to conduct operations autonomously, engaging targets without human intervention. This represents a significant deviation from traditional warfare ethics and raises profound concerns over the adherence to the principles of distinction and proportionality. Human Rights Watch has documented instances where such autonomous operations have led to civilian casualties, underscoring the critical need for MHC to mitigate these risks and ensure that AWS operations do not violate international humanitarian standards. The situation in Nagorno-Karabakh[50] also highlights the challenges and ethical implications of AWS deployments. These drones, capable of identifying and engaging targets based on algorithms, have conducted strikes in highly

[47] R. Moyes (2016), *Key Elements of Meaningful Human Control*.
[48] A-M. Eklund (2020), *Meaningful Human Control of Autonomous Weapon Systems*.
[49] [49] D. Hambling (2023), *Ukraine's AI Drones Seek and Attack Russian Forces Without Human Oversight*.
[50] D. Hambling (2020), *The 'Magic Bullet' Drones Behind Azerbaijan's Victory Over Armenia*.

complex environments. The lack of human oversight in these decisions poses serious risks to civilian safety and violates the principles of human dignity and ethical warfare. The deployment of AWS under such conditions highlights the critical need for MHC as a safeguard against the ethical breaches observed in these conflicts. Ensuring human oversight is paramount not only for maintaining legal compliance but also for preserving the integrity and humanity of warfare practices. By integrating MHC, we can uphold the ethical standards that govern military engagements and prevent the erosion of these core values, even as technological advancements continue to reshape the battlefield.

To bridge these practical examples with the broader discussion on stakeholder advocacy, it is essential to understand the critical perspectives brought forward by major advocacy groups. The Campaign to Stop Killer Robots and Article 36 have been instrumental in shaping the discourse around AWS by emphasizing the crucial need for stringent controls and human oversight. Their insights into the ethical ramifications of AWS deployment resonate deeply with the observed outcomes in conflict zones such as Ukraine and Nagorno-Karabakh, where the absence of MHC has led to significant ethical breaches. As we transition from examining the real-world impacts to the roles of these advocacy groups, it becomes clear that their concerns and proposed standards are not just theoretical but are grounded in urgent, practical realities. These groups advocate for a reevaluation and strengthening of the ethical frameworks governing AWS to prevent the kind of unintended consequences seen in these conflicts, highlighting the indispensable role of MHC in aligning AWS operations with international legal and ethical standards. As highlighted earlier, the Campaign to Stop Killer Robots[51] has been at the forefront of advocating for a ban on fully autonomous weapons. They argue that such systems lack the necessary human judgment required for complex combat situations, risking severe breaches of IHL and the dehumanization of military engagement. Similarly, Article 36[52] advocates for clear legal frameworks that mandate human control over lethal decision-making in military technologies. Their publications underscore the risks of permitting AWS to operate independently, particularly highlighting the potential violations of the principles of distinction, proportionality, and necessity—cornerstones of IHL. Article 36 asserts that without MHC, AWS cannot adequately assess the context of combat environments, which could lead to indiscriminate harm to civilians and disproportionate responses to military threats. They propose specific standards for the development, deployment, and use of AWS, including

[51] A-M. Eklund (2020), *Meaningful Human Control of Autonomous Weapon Systems*.
[52] R. Moyes (2016), *Key Elements of Meaningful Human Control*.

measures such as pre-engagement human analysis and decision-making checks to ensure that all actions taken by AWS are reviewed and accountable to human operators. By advocating for these principles, both the Campaign to Stop Killer Robots and Article 36 emphasize the essential role of human oversight not just for legal compliance but as a fundamental component of maintaining ethical integrity in warfare. Their ongoing efforts significantly inform international debates and help shape policies that aim to govern the use of AWS, ensuring these emerging technologies are integrated into military arsenals in a way that upholds both human dignity and international legal standards.

Each of these discussions, from the ethical implications to the real-world impacts of AWS deployments, underscores the indispensable role of MHC in aligning technological capabilities with ethical warfare practices. This exploration sets the stage for further examination of the roles and responsibilities of key stakeholders, diving into how developers, international bodies, and collaborative efforts shape the operational integrity and compliance of AWS with ethical and legal standards. While the ethical dimensions of MHC underscore the necessity of upholding principles like distinction, proportionality, and human dignity, these ideals cannot be fully realized without addressing the operational complexities of AWS deployment. Ethical compliance in autonomous warfare is not only a matter of moral judgment but also of technical precision and accountability mechanisms embedded in these systems. As such, bridging the gap between ethical imperatives and operational realities requires a thorough examination of the challenges posed by the design, deployment, and oversight of AWS in real-world scenarios. The following section explores these operational challenges, focusing on the technical reliability of AWS, the role of human judgment, and the frameworks needed to ensure ethical decision-making under complex and dynamic combat conditions.

2.2. Stakeholder Responsibilities and Challenges in Implementing MHC over AWS

Developers and operators of AWS are at the forefront of defining the ethical and operational boundaries within which these technologies operate. Their responsibilities are not merely technical but deeply ethical, influencing how AWS are perceived and utilized in combat scenarios. At the design stage, developers are tasked with incorporating MHC principles into AWS. This involves ensuring that the systems can make decisions that align with ethical

warfare standards. For instance, Paul Scharre[53] highlights the importance of designing AWS so that they can accurately assess the combat environment in order to comply with the laws of war. This means systems must be capable of distinguishing between combatants and non-combatants and assessing the proportionality of an attack, thereby preventing unnecessary harm. Integrating these capabilities during the development phase requires a thorough understanding of both technological possibilities and ethical imperatives. The concept of operational integrity[54] refers to the safeguard that AWS will function as intended in varying conditions without unintended consequences.

This integrity is contingent upon continuous human oversight and the ability to intervene or deactivate the system if it operates contrary to ethical or legal expectations. Developers must create mechanisms that allow for this level of control and transparency, ensuring that AWS actions are always accountable to human operators. At the development stage, developers must equip AWS with advanced sensors and algorithms that can discern intricate details in chaotic environments to prevent unlawful engagements. For instance, this might involve incorporating fail-safes that require human confirmation before engaging targets in ambiguous situations. This layer of human oversight ensures that AWS don't act solely based on algorithmic data, but also considers human judgment and accountability. Furthermore, Scharre emphasizes that the commitment to ethical design must be continuous and robust, involving rigorous testing and validation phases that simulate real-world scenarios to ensure that AWS behave as intended under all conditions[55]. This ongoing process helps identify any potential ethical breaches or operational failures before full-scale deployment. The dual responsibility of developers and operators, therefore, is not only to construct systems that can execute missions effectively but also to ensure that each mission adheres to ethical guidelines and legal frameworks established by international bodies. The rigorous application of MHC principles at every stage of AWS development and deployment is crucial. It mitigates the risk of misuse of such powerful technologies and upholds the core principles of distinction and proportionality as mandated by IHL, ensuring that every deployment of AWS aligns with enduring moral and ethical values.

As we shift our focus from individual responsibilities at the developmental stage to collective inputs from international bodies, we examine how these groups influence and standardize the implementation of MHC across different jurisdictions and contexts. The role of international

[53] P. Scharre (2016), *Autonomous Weapons and Operational Risk*.
[54] Ibid., p. 8-18.
[55] Ibid., p. 49-52.

and legal stakeholders, particularly bodies such as the United Nations Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems (LAWS) and the ICRC, is crucial in shaping the global discourse and standards for MHC compared to AWS[56]. These entities contribute significantly to the development of international guidelines that aim to ensure AWS operations are consistent with IHL. The GGE on LAWS, under the auspices of the UN CCW, has been instrumental in discussing the regulatory frameworks necessary for overseeing AWS. Their deliberations focus on key principles such as distinction, proportionality, and necessity – core elements of IHL that must guide the deployment of AWS to prevent unlawful harm. For instance, the GGE has explored various aspects of MHC, debating the extent of human judgment required in the decision-making process of AWS to ensure actions remain within legal and ethical boundaries. The outcomes of these meetings, including position papers and state submissions, provide a comprehensive overview of the international consensus (or lack thereof) on how to integrate MHC while preserving human oversight effectively.

Similarly, the ICRC has consistently advocated for clear legal standards governing the use of AWS, emphasizing the importance of maintaining human control to protect civilians in armed conflict scenarios. The ICRC's guidelines and recommendations[57] often stress the need for systems to allow human operators to override or deactivate AWS if they threaten to act contrary to established IHL principles. Their contributions are grounded in extensive field experience and legal expertise, ensuring that practical, ethical, and legal considerations inform discussions on MHC. These stakeholders also participate in shaping and endorsing international declarations and guidelines, such as the political declarations and guiding principles affirmed during CCW meetings. For example, the 2019 GGE on LAWS under the CCW[58] adopted a set of guiding principles. These principles, reflective of a broad international consensus, include clauses that emphasize human responsibility for decisions on the use of lethal force and the need for human-machine interaction to ensure compliance with international law. Such documents outline the shared responsibilities of states and developers implementing MHC systems that are robust, transparent, and accountable, thereby fostering a unified approach to regulating AWS on a global scale. The 2019 GGE report, for instance, explicitly calls for the

[56] CCW GGE on LAWS (2019), *Report of the 2019 session of the GGE on Emerging Technologies in the Area of AWS.*
[57] ICRC (2022), *ICRC Position on Autonomous Weapon Systems*.
[58] UN (2019), *Guiding Principles Affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems.*

consideration of human oversight mechanisms in the development and deployment of new weapons systems, ensuring that AWS actions are always subject to human judgment and control. Building on the foundational principles discussed by international and legal stakeholders, such as the UN GGE on LAWS and the ICRC, the next step involves actualizing these frameworks through global collaboration. These entities emphasize the need for stringent human oversight, setting the stage for various nations and organizations to unite and standardize the practices of MHC across the board. On the collaborative front, the importance of international cooperation in standardizing practices of MHC over AWS cannot be overstated. The CCW has hosted multiple rounds of discussions, where states, military experts, and human rights organizations converge to debate and shape the future of AWS regulation. The 2023 Meetings of the GGE on LAWS under the CCW have been pivotal. In these sessions, the discussions were deeply immersed in the complexities of operationalizing MHC, moving beyond theoretical models to address practical implementation challenges. For instance, Germany has established a regulatory sandbox[59] environment to test AWS under controlled conditions, assessing their compliance with IHL principles. These iterative processes aim to refine the mechanisms to ensure they meet the operational realities and ethical standards required for AWS deployments. The 2024 Meetings[60] emphasized the importance of creating robust feedback mechanisms to continuously improve the guidelines based on the outcomes of pilot programs and field experiences. This approach ensures that the protocols evolve in response to practical challenges and technological advancements in AWS. The outcomes of these discussions have led to enhanced guidelines that emphasize the critical role of human oversight in the deployment of AWS. Such collaborative efforts are vital for crafting a unified global response to the challenges posed by AWS, preventing technology from outpacing established ethical and legal frameworks. Through such international engagements, stakeholders collectively work towards a unified strategy for the responsible deployment of AWS in military operations, striving to align rapid technological innovations with established moral and legal frameworks.

While the international community has made progress in discussing the regulation of AWS, several critical challenges hinder efforts to achieve robust and universally accepted standards. First, resistance from some nations to stringent regulations poses a significant obstacle. Countries with advanced robotics and AI technologies may perceive strict regulation as a

[59] Federal Ministry for Economic Affairs and Climate Action (2022), *Regulatory Sandboxes – Testing Environments for Innovation and Regulation*.
[60] In 2024, the GGE met for 10 days in Geneva from 4-8 March and 26-30 August, to discuss about measures needed to ensure compliance with IHL concerning LAWS.

limitation on their strategic and military capabilities. For example, major powers like the United States and Russia have expressed reservations about binding treaties that might constrain their technological advancements or tactical flexibility in deploying AWS [61]. Technological challenges also play a critical role in complicating compliance with proposed regulations. The rapid pace of advancement in AI and robotics can outstrip the slower processes of diplomatic negotiation and international lawmaking. As a result, a persistent gap exists between the emerging capabilities of AWS and the existing legal and ethical frameworks designed to regulate them. This gap not only makes compliance challenging but also raises questions about the efficacy of regulations in keeping pace with technological evolution.

Furthermore, the political and strategic interests of states often complicate the adoption and enforcement of MHC principles. Strategic interests can lead to a reluctance to share critical technological information that is necessary for comprehensive international oversight. This secrecy can undermine efforts to develop a cohesive global strategy for AWS regulation. Additionally, geopolitical rivalries and the pursuit of national security objectives can override the international community's desire for consensus, leading to fragmented and sometimes contradictory approaches to AWS regulation[62]. These factors converge to create a complex and often contentious international environment where the ideal of uniform MHC standards confronts the realities of national interests and technological heterogeneity. The result is a regulatory landscape characterized by voluntary guidelines rather than binding agreements, with significant variations in how different countries implement MHC principles. This situation not only challenges the effectiveness of international norms but also raises concerns about the future of warfare, where autonomous technologies could operate in legally grey zones, potentially leading to escalations and violations that the current framework is ill-equipped to prevent or address.

2.3. Navigating Operational Challenges in AWS: Implementing MHC for Ethical and Legal Alignment

The deployment of AWS in complex and volatile combat environments raises significant challenges related to technical reliability and decision-making. As highlighted by Daniele

[61] A-M. Eklund (2020), *Meaningful Human Control of Autonomous Weapon Systems*.
[62] A-K. Ferl (2023), *Imagining Meaningful Human Control: Autonomous Weapons and the (De-) Legitimisation of Future Warfare*.

Amoroso and Guglielmo Tamburrini[63], AWS must operate with precision to ensure compliance with the core principles of IHL. However, achieving this alignment is far from straightforward. The unpredictability of real-world combat scenarios introduces variables that often exceed the programmed capabilities of AWS, exacerbating the risks of unintended engagement and legal violations.

2.3.1. Operational Unpredictability in Complex Environments

AWS rely on sophisticated algorithms and machine learning models to identify targets, assess threats, and execute actions autonomously[64]. However, these systems are limited by the quality of their training data and the constraints of preprogrammed logic. In highly dynamic environments, such as urban battlefields or contested airspaces, AWS face challenges like poor visibility, signal interference, and rapidly changing tactical landscapes. These factors undermine the accuracy of sensors and the ability of algorithms to discern between combatants and non-combatants. The SIPRI identifies these operational deficiencies as critical obstacles to ensuring that AWS meet the stringent demands of proportionality and distinction. Moreover, AWS decision-making processes often lack transparency, a phenomenon known as 'algorithmic opacity'[65]. This refers to the difficulty in understanding or predicting how an autonomous system will behave under specific conditions. For instance, adversarial countermeasures, such as spoofing or jamming, can disrupt AWS sensors, leading to erratic behavior. The inability to anticipate and interpret these malfunctions undermines trust in AWS and complicates accountability in the event of unlawful engagements.

2.3.2. Systemic Failures and the Theory of 'Normal Accidents'

Paul Scharre[66] introduces the concept of 'normal accidents' to describe the inevitability of failures in highly complex systems, such as AWS. Unlike simpler systems, where errors can often be isolated and rectified, the interdependent components of AWS create cascading risks. For example, a sensor malfunction might lead to incorrect data input, triggering a chain reaction of flawed decision-making that ultimately culminates in the unlawful use of force. Scharre

[63] D. Amoroso and G. Tamburrini (2021), *Toward a Normative Model of Meaningful Human Control Over Weapons Systems*.
[64] Ibid., p.252-253.
[65] J. Kwik and T. Van Engers (2021), *Algorithmic fog of war: When lack of transparency violates the law of armed conflict.*
[66] P. Scharre (2016), *Autonomous Weapons and Operational Risk*.

argues that these failures are not anomalies but inherent to the nature of autonomous systems, making robust fail-safes and human oversight mechanisms indispensable. Operational challenges are further intensified by AWS's inability to adapt to unforeseen scenarios. Machine learning models, although capable of processing vast amounts of data, often lack the contextual understanding necessary for nuanced decision-making. For example, AWS may fail to recognize civilian presence in complex environments, such as markets or evacuation zones, where the distinction between civilians and combatants is fluid. These limitations underscore the need to retain human judgment as a safeguard against erroneous or unethical actions.

2.3.3. Embedding MHC Across the AWS Lifecycle

MHC is indispensable for addressing the inherent unpredictability and operational risks associated with AWS. It serves as a critical operational mechanism that ensures AWS operate within ethical and legal boundaries by integrating effective human oversight. Lena Trabucco[67] emphasizes that MHC must be integral throughout the design phase, testing, deployment, and eventual deactivation. This comprehensive lifecycle approach is crucial for mitigating the risk of autonomous systems operating without adequate human input, particularly in volatile and complex combat scenarios where real-time decision-making is essential. MHC's operationalization begins with rigorous, iterative testing and simulation phases during the development of AWS. These phases simulate diverse combat scenarios, such as urban warfare or environments with limited visibility, or contested airspaces, allowing developers to assess and refine the reliability of AWS algorithms under varied scenarios. Trabucco underscores that such rigorous testing is vital to ensure that AWS algorithms align with the core principles mandated by IHL. For instance, AWS should require explicit human confirmation before engaging targets in ambiguous situations where misidentifications could lead to civilian casualties. This not only enhances ethical compliance but also minimizes the potential for unlawful engagements in real-world applications.

[67] L. Trabucco (2023), *What Is Meaningful Human Control, Anyway? Cracking the Code on Autonomous Weapons and Human Judgment*.

2.3.4. Real-Time Monitoring and Fail-Safes

However, the lifecycle approach does not end with deployment. Real-time human monitoring[68] systems play a critical role in ensuring continuous oversight during AWS operations. These systems must allow operators to intervene immediately if the system deviates from its expected behavior. Fail-safes, such as kill-switch mechanisms, are crucial for deactivating AWS in the event of malfunctions or when imminent ethical and legal breaches are likely. This ensures that human judgment remains central even in high-stakes, fast-paced combat environments. Paul Scharre [69] advocates for a dual-layered approach to MHC. The first layer involves the incorporation of fail-safes that empower human operators to override or deactivate AWS systems when errors or malfunctions are detected. These safeguards must be designed for speed and reliability, allowing immediate intervention without compromising the operational tempo of military engagements. Scharre aligns this approach with the precautionary principle, a critical tenet of IHL, ensuring that human operators retain ultimate control to prevent the escalation of unlawful or disproportionate actions. The second layer involves the implementation of 'human-in-the-loop' (HITL) or 'human-on-the-loop' (HOTL) models as foundational frameworks for implementing MHC[70]. In HITL models, human operators retain control over critical decisions, such as target selection and engagements, thereby ensuring accountability and adherence to ethical standards. HOTL systems, on the other hand, allow AWS to operate with a degree of autonomy while human supervisors monitor operations in real-time and intervene when necessary. Both approaches reflect a fundamental commitment to incorporating human oversight into AWS operations, striking a balance between the benefits of autonomy and the imperative for ethical accountability.

2.3.5. Accountability and Responsibility Tracing

The operationalization of MHC also demands robust accountability frameworks. AWS decision-making pathways must be designed to trace every action back to a human operator or supervisory chain, ensuring transparency and clear attribution of responsibility. This traceability is critical not only for ensuring compliance with IHL but also for addressing legal and moral accountability in cases of misconduct or failure. Trabucco's analysis[71] underscores

[68] P. Scharre (2016), *Autonomous Weapons and Operational Risk*.
[69] Ibid., p.42.
[70] Ibid., p.43.
[71] Lena Trabucco (2021), *Humanity in War? The Importance of Meaningful Human Control for the Regulation of Autonomous Weapons Systems.*

that without clear attribution of responsibility, the deployment of AWS risks undermining trust in both the technology and the legal frameworks governing its use.

2.3.6. Human Limitations and the Risk of Automation Bias

While MHC provides a safeguard against unethical or unlawful actions, its practical implementation presents significant challenges. Critics argue that the pace and complexity of AWS decision-making can outstrip the ability of human operators to respond effectively. For example, autonomous systems can execute multiple operations within milliseconds, leaving little room for human intervention in HOTL configurations. This issue is exacerbated in high-stress combat environments where operators may already be overwhelmed with information. Another concern is the reliance on robust technological infrastructure and situational awareness, which may not always be available in contested or resource-limited environments. Additionally, the risk of 'automation bias'[72] poses a significant threat, where operators over-rely on AWS capabilities, mistakenly assuming the system's algorithms are infallible. This overconfidence can lead to a dangerous erosion of vigilance and accountability, particularly in scenarios where AWS actions involve ethically questionable decisions. Trabucco and Scharre both emphasize that HITL configurations, while slower, remain the gold standards for ensuring MHC in life-and-death decisions. These configurations place human judgment at the center of AWS operations, maintaining accountability and ethical integrity even in high-pressure scenarios. However, as AWS technologies evolve, the strategies for incorporating MHC must evolve as well. Continuous refinement of control mechanisms, iterative testing, and the integration of advanced monitoring systems are essential to ensure that human oversight remains an adequate safeguard against the risks posed by autonomous military systems.

2.3.7. Technological Innovations to Support MHC

Innovative strategies and technological advancements are pivotal in enhancing the practical application of MHC in AWS. These innovations aim to address the dynamic challenges posed by autonomous operations while ensuring that AWS align with ethical and legal standards, particularly those established under IHL. Jeroen van den Boogaard[73] highlights the role of advanced sensors and adaptive algorithms as key to improving AWS's situational awareness.

[72] P. Scharre (2016), *Autonomous Weapons and Operational Risk*, p.32.
[73] J. Van Den Boogaard (2016), *Proportionality and Autonomous Weapons Systems*.

These technologies enable AWS to process complex and rapidly changing data inputs more effectively, which is crucial for adhering to the principles of proportionality and distinction. Improved sensing mechanisms, for example, can enable AWS to more effectively distinguish between combatants and non-combatants in densely populated or ambiguous environments, thereby reducing the risk of unlawful engagements.

Van den Boogaard also emphasizes the importance of integrating real-time decision-support tools into AWS to assist operators in high-pressure scenarios. These tools enhance the interpretability of AWS outputs, allowing operators to make informed judgments about the system's recommendations. One groundbreaking innovation in this context is the concept of "centaur warfighting," proposed by Paul Scharre[74]. This hybrid model combines human judgment with the efficiency of machine processing, ensuring that humans remain integral to decision-making processes while leveraging the speed and precision of AI systems. In centaur warfighting, AWS execute routine and time-sensitive tasks while deferring critical decisions—such as target selection and engagement—to human operators[75]. Regulatory sandboxes, such as those implemented in Germany, provide controlled environments for testing these hybrid models under ethical and legal constraints. Simulated real-world combat scenarios in these sandboxes allow developers and policymakers to assess AWS reliability and ethical compliance, identifying and addressing potential risks before deployment. Experts like Lena Trabucco[76] advocate for integrating predictive analytics into AWS systems to anticipate potential system errors, ethical breaches, or operational anomalies before they occur. For instance, by analyzing patterns in AWS data and environmental variables, predictive systems could flag high-risk situations, prompting operators to adjust AWS parameters or deactivate the system altogether.

2.3.8. Training and Dynamic Feedback in AWS Oversight

This preemptive approach mitigates the risk of unintended harm and enhances the overall reliability of AWS. Scharre[77] further emphasizes the need for dynamic feedback loops between AWS and human operators. These feedback mechanisms enable continuous updates to AWS operational parameters based on real-time data, ensuring adaptability to battlefield changes while maintaining alignment with IHL principles. For instance, in the event of an unexpected

[74] P. Scharre (2016), *Autonomous Weapons and Operational Risk*.
[75] Ibid., p. 41-49.
[76] L. Trabucco (2023), *What Is Meaningful Human Control, Anyway? Cracking the Code on Autonomous Weapons and Human Judgment*.
[77] P. Scharre (2016), *Autonomous Weapons and Operational Risk*, p. 38-40.

civilian presence in a combat zone, the feedback loop allows AWS to adjust its targeting parameters or pause operations until human input is received. Another critical element is the role of human operators in ensuring MHC. Enhanced training programs that focus on ethical decision-making and AWS-specific protocols are essential to ensure that human involvement in AWS operations is both meaningful and effective[78]. These training initiatives should emphasize the complexities of modern warfare, the operational limitations of AWS, and the principles of IHL. By equipping operators with a nuanced understanding of AWS capabilities and ethical constraints, these programs can mitigate risks associated with automation bias—the tendency of operators to over-reliance on AWS systems, assuming their decisions are infallible. Moreover, training programs must prepare operators for high-pressure scenarios that require rapid decision-making. Simulated exercises, similar to those conducted in regulatory sandboxes, can provide operators with hands-on experience in managing AWS under various conditions. This experiential learning is crucial for developing the situational awareness and judgment needed to intervene effectively when AWS systems deviate from expected behavior.

2.3.9. Continuous Improvement and Adaptive Learning Frameworks

Finally, iterative feedback mechanisms[79], as emphasized in recent discussions under the CCW, are indispensable for the continuous improvement of AWS protocols. These mechanisms allow AWS systems to evolve based on lessons learned from real-world deployments, ensuring that they remain responsive to technological advancements and operational challenges. For instance, post-deployment reviews can analyze AWS performance in specific engagements, identifying areas for improvement in both the system's technical capabilities and its integration with human oversight. Looking ahead, Jeroen van den Boogaard also emphasizes the importance of incorporating adaptive learning frameworks within AWS systems to enhance their responsiveness to evolving combat scenarios[80]. By allowing AWS to adjust its operational parameters based on real-time battlefield feedback, these frameworks ensure that the systems remain responsive while adhering to ethical constraints. This adaptability, paired with robust human oversight, is key to achieving a balance between technological innovation and the fundamental values of IHL.

---

[78] D. Amoroso and G. Tamburrini (2021), *Toward a Normative Model of Meaningful Human Control Over Weapons Systems*.
[79] H-M. Roff, and R. Moyes (2016), *Meaningful Human Control, Artificial Intelligence and Autonomous Weapons.*
[80] J. Van Den Boogaard (2016), *Proportionality and Autonomous Weapons Systems*.

2.4. Concluding Remarks

This chapter has explored the multifaceted ethical, legal, and operational challenges posed by the deployment of AWS in modern warfare, with a focus on the pivotal role of MHC in mitigating these issues. Ethical concerns, such as potential breaches of the principles of distinction and proportionality under IHL, were analyzed through real-world examples like Ukraine and Nagorno-Karabakh, underscoring the human cost of unregulated AWS. Operationally, the discussion highlighted technical limitations, algorithmic opacity, and the inherent unpredictability of complex combat environments, which compromise the reliability and accountability of AWS. In particular, MHC was presented as a safeguard, offering frameworks such as HITL and HOTL models to ensure ethical oversight while leveraging technological advancements. The insights from this chapter pave the way for further exploration of MHC's practical implementation and policy implications. Henrik Syse[81] emphasizes that the integration of ethics and law must underpin all governance models for AWS. Future research should focus on standardizing MHC definitions across international frameworks, addressing ambiguities that undermine consensus and enforcement. Policy development must prioritize adaptive guidelines that evolve in tandem with technological innovations, ensuring that MHC remains a dynamic and enforceable principle. Collaborative regulatory approaches, like those led by the CCW, are vital in aligning global perspectives on AWS governance.

Additionally, the role of accountability frameworks in attributing responsibility for AWS actions needs to be clarified, thereby bridging gaps in legal and moral liability. Comprehensive, universally accepted guidelines for MHC are essential to harmonize ethical and operational standards for AWS. Clear definitions that encapsulate the principles of distinction, proportionality, and necessity are imperative for compliance with IHL and broader human rights norms. Syse's assertion that conflict itself must be controlled through fairness, ethics, and law underscores the importance of robust MHC protocols. These guidelines should not only address technological requirements but also incorporate the socio-political dynamics that influence AWS deployment, ensuring that both human and machine actions uphold the values of humanity and justice. The conclusion of this chapter reaffirms MHC's centrality in bridging the gap between rapid technological advancements and enduring ethical values. By integrating the principles outlined here into future research, policy frameworks, and operational strategies,

[81] H. Syse (2023), *Meaningful Human Control*

the international community can ensure that AWS contribute to enhancing security and upholding justice, rather than exacerbating the complexities of modern warfare.

Chapter 3. From Supervision to Responsibility: Building the Foundations of MHC in AWS

The previous chapters have established the critical role of MHC in governing AWS. Expanding on this foundation, this chapter dissects the key elements of MHC – human supervision, context control, and accountability – to assess their role in ensuring compliance with IHL and ethical military conduct. This analysis examines the technical and procedural mechanisms necessary for maintaining human oversight, particularly in decision-making processes where autonomous systems operate in dynamic combat environments. The ICRC[82], in its position paper, warns of the risks associated with diminished human oversight in AWS, particularly concerning adherence to the principles of distinction and proportionality[83], which are essential under IHL. Article 36 of AP I to the Geneva Conventions[84] further mandates that new weapons undergo thorough legal reviews to ensure compliance with international law, reinforcing the necessity of human supervision and contextual control as integral elements of AWS governance. The absence of strong MHC frameworks raises concerns about accountability gaps in AWS deployments, posing challenges for both military command structures and broader public oversight.

This chapter addresses the sub-question: "*How does meaningful human control contribute to accountability in the deployment of AWS?".* By examining human supervision mechanisms, context control in operational decision-making, and accountability structures, this analysis provides insight into the procedural safeguards necessary to maintain human oversight in AWS operations. Real-world examples underscore the risks posed by insufficient MHC, Frank Sauer[85] highlights the dangers of AWS escalating conflicts and unpredictability, while Maciek Zajac[86] demonstrates how failures in MHC have led to unintended engagements and civilian

[82] ICRC (2022), *ICRC Position on Autonomous Weapon Systems*.
[83] N. Davidson (2018), *A Legal Perspective: Autonomous Weapon Systems under International Humanitarian Law.*
[84] V. Boulanin (2015), *Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems.*
[85] F. Sauer (2021), *Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible*.
[86] M. Zajac (2023), *AWS Compliance with the Ethical Principle of Proportionality: Three Possible Solutions*.

casualties. These cases illustrate how the erosion of human control can lead to legal and ethical violations, underscoring the need for robust frameworks to trace responsibility back to human agents.

The discussion unfolds in three key areas. First, it examines frameworks for human supervision and accountability, including authorization protocols and oversight mechanisms that ensure AWS actions remain under human control. Then, it explores context control and operational decision-making, analyzing how ethical and legal constraints must shape AWS behavior in battlefield scenarios. Finally, it considers the chain of responsibility and public accountability, highlighting the importance of transparency in ensuring AWS compliance with both military accountability structures and broader international norms. Each of these sections contributes to a comprehensive assessment of MHC, offering insights into how AWS regulations can be strengthened through technical, legal, and procedural safeguards. By bridging technological advancements with ethical principles, this chapter supports the thesis's broader goal of defining and operationalizing MHC in a way that reinforces international accountability standards and ensures the responsible deployment of autonomous weapons.

3.1. Ensuring Human Oversight: Supervision, Authorization, and Accountability in AWS

Human supervision serves as a critical governance mechanism within AWS, fundamentally necessary to ensure adherence to IHL and the preservation of ethical military conduct. The ICRC emphasizes the crucial role of robust human oversight[87], particularly in mitigating risks associated with AWS operations that may otherwise contravene the IHL principles of distinction and proportionality. According to the ICRC, without stringent human control, AWS might engage targets indiscriminately, violate non-combatant immunity, and potentially cause disproportionate civilian harm, thereby breaching core humanitarian principles[88]. To strengthen human oversight, advanced decision-support systems are pivotal. These systems are designed to enhance human operators' capabilities by providing real-time data integration and AI-driven analytics. Such technological enhancements enable operators to achieve improved situational awareness and decision-making precision, thereby facilitating more informed and ethically

[87] ICRC (2022), *ICRC Position on Autonomous Weapon Systems*.
[88] Ibid.

aligned interventions. For example, systems equipped with cognitive interfaces[89] can analyze vast arrays of sensor data to highlight ethical considerations and propose action courses that comply with legal standards, thus bridging the gap between human judgment and machine execution. One notable application of these technologies is the Israeli Defense Forces' use of advanced command-and-control systems, which require operator confirmation for sensitive target engagements, ensuring that each military action is deliberate and legally justified[90]. These technological frameworks ensure compliance with stringent ethical and legal standards while also bolstering accountability by maintaining a transparent human command chain over AWS's autonomous functions. By embedding human operators within the operational loop, these systems reflect the principles of MHC, directly aligning with this thesis's goal to define and operationalize MHC within AWS regulatory frameworks. They ensure AWS operations are both practical and ethical, as well as reversible and justifiable, adhering to international accountability norms.

Building on the foundation of robust human supervision, authorization protocols[91] play a crucial role in embedding MHC and enhancing accountability within AWS operations. These protocols ensure that every action executed by AWS is explicitly authorized by a human operator, thereby establishing a transparent and traceable command structure. This traceability is crucial for maintaining operational integrity and preventing unauthorized autonomous actions that could lead to unintended consequences. The U.S. DoD outlines these protocols in its DoD Directive 3000.09[92], which mandates human involvement in the deployment and use of autonomous and semi-autonomous weapon systems. The directive emphasizes that "appropriate levels of human judgments"[93] shall be exercised before to the deployment of weapon systems to perform their intended functions, thereby ensuring that critical decisions remain under human control and are subject to rigorous oversight. In practice, these authorization protocols are intended to integrate coherently with established command-and-control structures, thereby enhancing the capacity of military commanders to oversee and control AWS deployments effectively. For instance, the directive stipulates the development of operational guidelines that require manual activation[94] of certain AWS functionalities,

[89] E. von Mühlenen et al. (2024), Regulating *the Future: Navigating Ethical and Legal Pathways in Brain-Computer Interface Technology.*
[90] M. Liebergall (2023), *New Investigations Detail Concerns Over Israel's Use of AI in Choosing Targets.*
[91] J. Kwik (2022), *A Practicable Operationalization of Meaningful Human Control.*
[92] U.S. Department of Defense (2023), *DoD Directive 3000.09 – Autonomy in Weapon Systems.*
[93] Ibid., p. 10.
[94] Ibid., p. 11.

particularly those involving the use of lethal force. This approach not only reinforces the role of human judgment in critical decision-making processes but also exemplifies the operationalization of MHC, aligning with international standards that demand accountability and proportionality in the use of force. By enforcing strict compliance with these authorization protocols, the military can ensure that all actions taken by AWS are justified and documented, thereby minimizing the risk of legal and ethical violations.

While robust authorization protocols are essential for immediate oversight and control of AWS operations, comprehensive legality reviews mandated by Article 36 of AP I to the Geneva Conventions[95] provide a critical secondary layer of scrutiny. These reviews are pivotal for validating that the design, development, and deployment of AWS are in strict adherence to IHL, particularly concerning the principles of distinction, proportionality, and military necessity[96]. Similarly, while the DoD Directive 3000.09[97] ensures that each action by AWS is deliberately authorized and controlled, Article 36 reviews assess broader compliance, ensuring that AWS systems, by their very design, can operate within these legal and ethical frameworks. This dual approach not only reinforces operational directives established through authorization protocols but also integrates a rigorous legal and ethical review process that evaluates the potential long-term implications of AWS deployment.

The 2019 report by the CCW Meeting of States Parties[98], highlights the importance of these reviews in ensuring that AWS can make real-time decisions that adhere to humanitarian standards. The rigorous nature of Article 36 reviews involves a comprehensive analysis of the weapon system's capabilities, targeting mechanisms, and decision-making algorithms to ensure they do not result in unlawful harm or unnecessary suffering[99]. This process is critical not only for compliance with the law of armed conflict but also for maintaining public and international trust in the deployment of advanced military technologies. There is a necessity for transparency[100] in these reviews. States must share review outcomes where possible to foster broader accountability and confidence in the ethical deployment of AWS. Furthermore, the

[95] Article 36 (2013), *Killer Robots: UK Government Policy on Fully Autonomous Weapons*.
[96] V. Boulanin (2015), *Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems.*
[97] U.S. Department of Defense (2023), *DoD Directive 3000.09 – Autonomy in Weapon Systems.*
[98] CCW (2019), *Guiding Principles Affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems.*
[99] D. Copeland et al. (2022), *The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems*.
[100] Ibid., p.293.

reviews are designed to identify any potential for AWS to act autonomously in ways that could contravene ethical norms, such as engaging targets without explicit human authorization. By requiring that AWS systems undergo these legal assessments, international law aims to prevent the deployment of systems that could perform indiscriminate attacks to distinguish adequately between combatants and non-combatants. The Article 36 reviews, therefore, serve to complement the immediate controls provided by authorization protocols, thereby forming an integrated framework that enhances accountability and ethical deployment of AWS.

Advancing beyond the foundational layer of robust authorization protocols, which ensure that each action by AWS is explicitly authorized and traceable, the integration of advanced technological systems further enhances this accountability framework. These systems, including real-time monitoring systems and decision-support tools, extend beyond mere compliance tools to strengthen the capacity of human operators[101]. They enable operators to dynamically supervise and refine AWS actions, aligning operations with evolving operational contexts and ethical standards. The deployment of these technologies ensures that AWS operations are not only controlled but also continuously monitored and adjusted. For instance, the use of interactive user interfaces and advanced algorithms capable of analyzing vast amounts of data in real-time enables operators to maintain a high level of oversight and control[102]. These systems are crucial for identifying potential ethical or legal issues, prompting human intervention before any critical decisions are executed. Furthermore, the integration of machine learning tools[103]that can predict probable outcomes based on previous engagements helps operators preemptively correct course and prevent breaches of legal and ethical conduct.

A hypothetical example of technology that could significantly enhance human supervision in AWS operations is sensor fusion systems[104]. These systems could theoretically integrate data from multiple sources to provide a comprehensive view of the battlefield, enhancing the operator's ability to distinguish between combatants and non-combatants and assess proportionality when deploying AWS. Moreover, the strategic incorporation of Article 36 reviews, as mandated by the Geneva Conventions, complements these technological advancements. These reviews are pivotal for validating that the design and deployment of AWS

[101] C. Miller et al. (2023), *Meaningful Human Control of AI-based Systems: Workshop Technical Evaluation Report, Thematic Perspectives and Associated Scenarios.*
[102] Y. Shany and R. Herring (2024), *Meaningful Human Control and the Autonomous Weapons Systems Debate*.
[103] Ch. P. Trumbull (2019), *Autonomous Weapons: How Existing Law Can Regulate Future Weapons.*
[104] P. Scharre (2018), *Army of None: Autonomous Weapons and the Future of War.*

adhere to the principles of distinction, proportionality, and military necessity, ensuring compliance with IHL[105]. This dual approach, combining immediate technological oversight with comprehensive legal reviews, fortifies the ethical and legal framework within which AWS operate. It ensures that every technological input and operational decision aligns with stringent international standards, thereby enhancing the accountability and integrity of military operations. This integration of advanced supervision tools with Article 36 legality assessments exemplifies the operationalization of MHC, advancing the thesis's objective of defining and operationalizing MHC within the regulatory framework of AWS operations.

Furthermore, it is essential to recognize that these technological integrations form just part of a broader accountability framework that extends into the realm of international military strategy and policy development. This emphasizes the invaluable insights from defense policy analysts and military strategists, whose expertise is crucial for evolving and refining AWS oversight mechanisms. Such strategic perspectives ensure that the technological capabilities extend beyond implementation, aligning with robust policy frameworks that enhance accountability and ensure compliance with ethical and legal standards. For instance, discussions held under the auspices of NATO on MHC illustrate the international commitment to establishing transparent and accountable command structures. These discussions often explore the challenges and solutions related to maintaining control over AWS, emphasizing the necessity for systems that allow for decisive human intervention at critical stages of weapon deployment. A key document from the NATO Science and Technology Organization, titled *'Meaningful Human Control of AI-based Systems: Workshop Technical Evaluation Report, Thematic Perspectives and Associated Scenarios,'* [106] provides detailed insights into these complex debates. It discusses how international military alliances are striving for a consensus[107] on protocols that ensure AWS operations comply with ethical standards and legal obligations. This international discourse is pivotal in shaping policies that govern the use and oversight of autonomous military technologies, aiming to align them with broader objectives of global security and humanitarian law.

The inclusion of contrasting views from entities like the SIPRI and the ICRC significantly enriches the discourse. SIPRI is recognized for its comprehensive research on global security

[105] V. Boulanin (2015), *Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems.*
[106] C. Miller et al. (2023), *Meaningful Human Control of AI-based Systems: Workshop Technical Evaluation Report, Thematic Perspectives and Associated Scenarios.*
[107] Ibid.

issues, including the implications of emerging military technologies[108]. Their work often highlights the potential risks and unintended consequences associated with the deployment of AWS, advocating for a more cautious approach to technology integration in military operations. On the other hand, the ICRC brings a humanitarian perspective, focusing on the protection of civilians in armed conflicts[109]. Their advocacy is rooted in the principles of IHL, which they argue must be central to the development and deployment of AWS to prevent violations such as indiscriminate attacks or excessive collateral damage. By incorporating these insights, the international dialogue becomes more robust, fostering the development of policies that strive for technological advancement and operational effectiveness, while also prioritizing ethical standards and legal compliance. This nuanced approach ensures that the governance of autonomous military technologies aligns with the broader objectives of maintaining international security and upholding humanitarian law, thereby directly contributing to the definition and operationalization of MHC.

This analysis has demonstrated the critical role of human supervision and robust authorization protocols in AWS operations, affirming the foundational importance of MHC in maintaining compliance with IHL and ethical military conduct. It further examined how advanced decision-support systems enhance oversight and how Article 36 reviews provide a secondary layer of scrutiny that aligns AWS design and operation with stringent legal and ethical frameworks. These insights highlight the complexity of integrating technological advancements with traditional military oversight mechanisms, illustrating the need for continuous evaluation and adaptation of policies governing the deployment of autonomous technologies. By operationalizing MHC through these frameworks, we contribute directly to the broader objectives of international security and the protection of humanitarian values, ensuring that AWS are deployed in a manner that is both effective and aligned with international accountability norms. Transitioning to the next section, the focus will shift from the overarching frameworks of supervision and accountability to more detailed aspects of how AWS are controlled within operational settings. This analysis will delve into the mechanisms that ensure AWS actions are consistent with operational goals and ethical considerations, further examining how these systems can be structured to respond dynamically to complex battlefield conditions while still maintaining strict compliance with ethical and legal standards. This

[108] V. Boulanin, et al. (2021), *Autonomous Weapon Systems and International Humanitarian Law: Identifying Limits and the Required Type and Degree of Human–Machine Interaction*.
[109] ICRC (2022), *ICRC Position on Autonomous Weapon Systems*.

progression from macro-level oversight to micro-level control mechanisms is pivotal in fully operationalizing MHC, building on the foundation established in this section, and advancing the thesis's goal of defining and implementing MHC within a comprehensive framework of AWS governance.

3.2. Operationalizing Context Control and Decision-Making in AWS: Bridging Strategic Oversight with Tactical Precision

In the preceding section, the overarching frameworks of supervision and accountability essential for governing AWS were explored. As the focus shifts from these broader themes to the more detailed aspects of AWS control within operational settings, it becomes imperative to focus on how these systems are managed on a day-to-day basis in dynamic and often unpredictable combat environments. This section explores the crucial mechanisms of context control and operational decision-making, pivotal elements in operationalizing MHC on AWS. The progression from macro-level oversight to micro-level control mechanisms is not merely a shift in focus but a necessary evolution in the governance of AWS. While overreaching frameworks set the stage for ethical and legal compliance, the actual implementation of these frameworks in operational settings determines their effectiveness in real-world scenarios. This transition is critical for ensuring that the theoretical foundations of MHC are translated into practical, actionable strategies that maintain human oversight at every level of AWS deployment. Integrating real-time analytics and AI-driven insights into operational decision-making is crucial, as it enables adjustments to dynamic combat environments. This ensures that decisions made by AWS are always informed by the most current situational awareness, aligning with ethical and legal standards. Emphasizing this transition highlights the nuanced challenges and responsibilities inherent in the management of micro-level controls. These include the need for precise and context-aware decision-making processes that can dynamically respond to the complexities of modern battlefields. This approach ensures that AWS operate within the strict boundaries set by international law and ethical guidelines, reinforcing the principles of proportionality, distinction, and military necessity as outlined in IHL. By focusing on the detailed mechanisms that enable effective control and decision-making at the operational level, this section aims to bridge the gap between high-level policy directives and their practical implementation. It underscores the importance of a coherent integration between strategic oversight and tactical control, which is essential for the successful operationalization of MHC within regulatory frameworks.

Context control in AWS refers to the system's ability to interpret and react to the complex dynamics of their environment in a manner that adheres to ethical and legal standards[110]. This capability is crucial for guiding operational decisions, ensuring that AWS actions remain within predefined ethical and legal parameters, which are essential for compliance with IHL and ethical military conduct. Operational decision-making in the context of AWS involves making real-time decisions based on data and situational awareness to achieve tactical objectives while adhering to legal and ethical standards[111]. Implementing context control in AWS presents significant challenges. A major challenge is the development of contextual awareness that enables AWS to assess and respond to rapidly changing battlefield scenarios accurately[112]. The difficulty lies in programming AWS to recognize subtle cues that human soldiers interpret instinctively, which is crucial for distinguishing between combatants and non-combatants or assessing the proportionality of an attack in real-time. Further complicating the implementation of context control is its integration into existing frameworks. Effective context control in AWS extends beyond the mere deployment of advanced technologies, it requires a comprehensive understanding of operational doctrine and the rules of engagement[113]. Real-time decision-making is enabled by integrating advanced decision-making algorithms that analyze live data from the battlefield, allowing for immediate and informed responses. Specific examples of machine learning models used in operational settings include decision trees[114] and neural networks[115], which process sensor data to enhance situational awareness and improve decision-making accuracy[116]. These models are crucial for real-time decision-making in complex battlefield scenarios. The necessity for AWS to be equipped with mechanisms that facilitate real-time data processing and decision-making is emphasized, reflecting both the immediate tactical situation and overarching strategic objectives.

After establishing the fundamental role of context control in guiding AWS to act within ethical and legal norms, it becomes essential to explore how this capacity is technically achieved. The

[110] J. Kwik (2022), *A Practicable Operationalization of Meaningful Human Control*.
[111] Ibid.
[112] Ibid., p.10.
[113] A-M. Eklund (2020), *Meaningful Human Control of Autonomous Weapon Systems*.
[114] Decision tree: a machine learning model that uses a tree-like graph of decisions and their possible consequences. It's used to go from observations about an item to conclusions about them item's target value. It's useful for classification tasks. / https://www.ibm.com/think/topics/decision-trees
[115] Neural networks: computational models inspired by the human brain's structure. They consist of layers of interconnected nodes (neurons), which process input data through various layers to produce output. They excel at recognizing patterns from complex datasets and are widely used in tasks like image and speech recognition. / https://www.ibm.com/think/topics/neural-networks
[116] Ch. P. Trumbull (2019), *Autonomous Weapons: How Existing Law Can Regulate Future Weapons.*

development of contextual awareness in AWS, while challenging, is facilitated through advanced sensor technologies and machine learning models. These technologies are pivotal in addressing the challenges of rapid environmental changes and the requirement for precise situational analysis. To navigate the complexities of modern battlefields, AWS are equipped with an array of sophisticated sensors. These arrays capture multimodal data[117], encompassing visual[118], infrared[119], and radar[120] sensors, each providing a unique perspective and vital information about the battlefield. The operational decision-making process utilizes this sensor data to make quick and informed decisions that are crucial for dynamic and rapidly evolving combat scenarios. The integration of these sensors involves sophisticated data fusion techniques. Data fusion[121] enables AWS to integrate information from these diverse sources into a comprehensive understanding of the environment. This process not only enhances the accuracy of target detection and identification but also significantly reduces the risk of misidentification. Advanced algorithms interpret this combined data, enabling AWS to make rapid and reliable decisions based on comprehensive situational analysis. MHC is critical here, as it ensures that despite the high level of autonomy, human judgment remains central to the decision-making process, particularly in ambiguous or ethically complex situations.

Beyond the integration of sensor data, the cognitive capabilities of AWS are significantly bolstered by advanced machine learning algorithms. These algorithms are central to AWS's decision-making processes, designed to analyze vast datasets and discern complex patterns of behavior that distinguish hostile actions from civilian activities[122]. This analysis is fundamental to operational decision-making, where split-second decisions can have significant implications. Utilizing techniques such as supervised learning[123], where models are trained on labeled datasets to recognize combatant versus non-combatant scenarios, AWS can refine their predictive accuracy over time. This training involves iterative reassessment and optimization based on new operational data, continually enhancing the system's decision-making precision.

---

[117] P.Scharre (2018), *Army of None: Autonomous Weapons and the Future of War.*
[118] Ibid. / Visual sensors: capture high-resolution imagery, useful for identifying visible features and movements. They are particularly effective in daylight operations, capturing fine details such as uniform patterns and vehicle markings, crucial for identifying combatant forces and distinguishing them from civilians.
[119] Ibid. / Infrared sensors: play a critical role in nighttime and obscured condition operations. They detect heat signatures from living bodies and mechanical sources, enabling AWS to identify and track human and vehicle targets even in low visibility conditions, such as smoke, fog, or complete darkness.
[120] Ibid. / Radar sensors: complements visual and IR sensors by providing reliable data through adverse weather and across various terrains. They can detect and track movements by emitting radio waves and analysing the reflected signals, making it indispensable for assessing the speed and direction of objects, which is vital for dynamic engagement scenarios.
[121] V. Boulanin et al. (2017), *Mapping the Development of Autonomy in Weapon Systems.*
[122] V. Boulanin et al. (2017), *Mapping the Development of Autonomy in Weapon Systems.*
[123] Ibid., p. 16.

Deep learning[124], a subset of machine learning, is particularly effective in processing high-dimensional data from various sensors. These deep neural networks [125] are capable of identifying subtle nuances in data that might elude traditional algorithms, enabling nuanced interpretations of complex environments. These capabilities are integral to the operational decision-making in AWS, ensuring that actions are taken based on comprehensive and accurate data analysis. For instance, convolutional neural networks (CNNs) [126] are used for image recognition tasks and can help AWS in visual data analysis to accurately identify and classify objects in both urban and rural battlefields. The ongoing learning process is vital not only for the system's accuracy but also for its reliability, as it helps to minimize errors and biases that could lead to civilian harm or other unlawful actions. Moreover, the ethical implications of deploying machine learning within AWS are mitigated through continuous human oversight. Human operators oversee the learning process, adjusting parameters and correcting courses as needed to align with ethical standards and rules of engagement[127]. This symbiosis between human judgment and automated processes ensures that AWS operations are conducted within a framework that prioritizes human dignity and adherence to international law, making meaningful human control a reality in the age of autonomous weaponry.

The integration of advanced sensor technologies and sophisticated machine learning models equips AWS with unparalleled capabilities for environmental awareness and decision-making accuracy. However, the reliance on these technologies introduces inherent challenges that must be navigated to ensure that AWS operations remain ethical and legally compliant. With the advanced capabilities of machine learning in AWS established, it is essential to explore the ethical considerations and limitations associated with algorithmic decision-making. These challenges necessitate a comprehensive strategy that includes robust algorithm design, regular updates, ethical audits, and the seamless integration of human oversight to maintain control and accountability [128]. The integration of operational decision-making processes within this framework is essential to ensure that tactical decisions made by AWS are timely, precise, and adhere to the highest standards of legal and ethical military conduct[129]. While AWS benefit

[124] Ibid., p. 17.
[125] Ibid., p. 17.
[126] C. Chow (2020), *Deep Learning for Aircraft Recognition Part I: Building a Convolutional Neural Network (CNN) from Scratch.*
[127] I. Bode and T.F.A. Watts (2023), *Loitering Munitions and Unpredictability: Autonomy in Weapon Systems and Challenges to Human Control.*
[128] A. Seixas Nunes (2022), *Autonomous Weapons Systems and Deploying States. Making Designers and Programmers Accountable*.
[129] J. Kwik (2022), *A Practicable Operationalization of Meaningful Human Control*.

from advanced algorithms that enhance their operational effectiveness, these algorithms can also be prone to biases and errors that may compromise regulatory adherence[130]. To mitigate these risks, AWS algorithms are engineered with robustness in mind, ensuring they perform reliably across a wide range of varied and unpredictable conditions. Regular updates and ethical audits are integral to this process, helping to refine these algorithms continuously and prevent them from perpetuating biases or executing unjustifiable actions. The integration of human oversight with AI operations is pivotal in managing the complexities of AWS. Operators are equipped with sophisticated interfaces that provide real-time data and actionable insights, enabling them to make informed and timely decisions[131]. This human-AI collaboration is essential not only for enhancing the operational capabilities of AWS but also for ensuring that every action taken by the system aligns with both tactical requirements and ethical imperatives. By fostering a symbiotic relationship between human operators and automated systems, AWS can operate within a framework that upholds the principles of MHC, ensuring that decisions are made with a high degree of ethical consideration and adherence to international law.

Implementing robust control mechanisms is crucial to ensure that AWS operations align with the established principles of IHL, particularly proportionality and distinction. MHC plays a pivotal role here, as it ensures that human judgment guides the evaluation and execution of AWS actions. By maintaining human oversight, MHC ensures that AWS can accurately assess operational environments and make decisions that adhere to legal norms, thereby safeguarding civilian populations and infrastructure during military engagements. The integration of advanced decision-making protocols within the operational frameworks of AWS ensures real-time adaptability and compliance with established IHL principles, essential for the effective management of military engagements. The advancement of AWS introduces significant complexities in attributing responsibility, particularly when failures in context control result in unintended or unlawful actions. As AWS become more autonomous, determining the source of accountability, whether it be the operators, commanders, or the designers of the systems, becomes increasingly challenging. This is where MHC becomes indispensable. MHC ensures that, despite the autonomy of AWS, there is always a clear line of human oversight and control that can be audited and held accountable. Establishing robust international laws and regulations

[130] F. Sauer (2021), *Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible.*
[131] Ch. P. Trumbull (2019), *Autonomous Weapons: How Existing Law Can Regulate Future Weapons*

that define clear standards and responsibilities for the use of AWS in accordance with the principles of MHC is crucial.

3.3. Building Responsibility and Trust Through Oversight and Transparent Command in AWS Operations

This section explores the intricate structure of accountability and responsibility that underpins the deployment of AWS within the MHC framework. As the capabilities of AWS evolve, ensuring that these systems operate within predefined ethical and legal parameters becomes crucial. The focus here shifts from the operational mechanisms discussed in previous sections to the safeguards that ensure the responsible and transparent use of these technologies. The discussion explores how MHC establishes a clear and enforceable chain of responsibility within military operations, outlining the roles and hierarchies that extend from strategic decision-makers to tactical operators. Every action is meticulously traced back to a human responsible for its authorization, thus securing the integrity of military operations in the eyes of both national and international observers. Additionally, the importance of public accountability is highlighted, emphasizing the need for transparency in AWS operations. Such openness is crucial for fostering trust between the military and the civilian population and for upholding that military practices align with international humanitarian standards. By examining how these frameworks operate in practice, this section underscores the crucial role of MHC in ensuring human oversight and accountability in the deployment of advanced military technologies.

Military accountability refers to the systems, processes, and structures that ensure all actions undertaken by armed forces are directed, documented, and evaluated through responsible command-and-control structures[132]. Within the context of AWS, implementing MHC is crucial. MHC mandates that human operators oversee and control the strategic and operational use of AWS and ensures that these systems comply with IHL. Integrating MHC enables the military to maintain human oversight over complex, automated technologies, which is crucial for ensuring operational integrity, legal compliance, and public trust. Enhancing traceability and command integrity within military operations that utilize AWS is a critical aspect of maintaining operational accountability and compliance with IHL[133]. In this context, the

[132] The Center of Ethical Education in the Armed Forces (2024), *Humanity in War? The Importance of Meaningful Human Control for the Regulation of Autonomous Weapons Systems.*
[133] D. Amoroso and G. Tamburrini (2021), *Toward a Normative Model of Meaningful Human Control Over Weapons Systems.*

Department of Defense's Directive 3000.09 on AWS provides a robust framework for integrating AWS into U.S. military operations[134]. The directives mandate that AWS operations incorporate "appropriate levels of human judgment"[135], ensuring that the autonomy of these systems does not override human decision-making processes, thereby maintaining a transparent chain of command and accountability. By doing so, it safeguards that every decision made by AWS is traceable and subject to human oversight, thereby ensuring that decisions are taken responsibly.

Similarly, discussions within NATO[136] regarding the MHC of AI-based systems highlight the alliance's commitment to a unified approach in the deployment of autonomous technologies. This standardization is intended to strengthen command structures and enhance accountability across international military operations, ensuring that universally accepted controls govern AWS actions and are transparent in their execution. By enhancing traceability and command integrity, initiatives such as the DoD Directive 3000.09 and NATO discussions on MHC are instrumental in promoting the responsible use of advanced military technologies and building trust among international partners and the public. By demonstrating how enhanced traceability and command integrity within the framework of MHC maintain the rigor of military standards, these frameworks ensure that AWS operations are confined within established military ethics and legal norms. This contributes to the broader goals of international peace and security while at the same time strengthening trust and accountability in military engagements globally.

A critical question in the operationalization of MHC concerns both the extent to which such control is exercised and the determination of who within the chain of command must hold it at each stage of an AWS's lifecycle. This issue has been addressed in various forms across policy, legal, and military guidance, including ICRC statements, NATO discussions, deliberations within the CCW GGE, and academic analyses. Across these discourses, there is broad recognition that responsibility for exercising MHC cannot rest in a single role, but must be systematically distributed throughout multiple levels of the military command structure. One structured approach to mapping this distribution is offered by the taxonomy developed by the InterAgency Institute from the 2024 CCW GGE sessions, which conceptualizes MHC along

[134] U.S. Department of Defense (2023), *DoD Directive 3000.09 – Autonomy in Weapon Systems.*
[135] Ibid., p.10.
[136] C. Miller et al. (2023), *Meaningful Human Control of AI-based Systems: Workshop Technical Evaluation Report, Thematic Perspectives and Associated Scenarios.*

the axes of "*who exercises control, over what, when, and how*"[137]. While this framework provides a structured analytical lens, comparable multi-level allocation models are also reflected in humanitarian, operational, and doctrinal guidance.

In this model, the responsibility for exercising MHC is distributed across multiple, interrelated levels of the military hierarchy. At the strategic level, senior commanders retain the authority to authorize the deployment of AWS in alignment with strategic objectives and the overarching obligations of IHL. Their responsibilities include defining mission parameters, rules of engagement, and operational constraints in a manner that ensures lawful and ethical deployment[138]. They must also ensure that systems selected for deployment are capable of predictable behavior within these parameters, and that a clear, traceable chain of accountability is maintained for every decision[139]. This responsibility is consistently reflected across military, humanitarian, and policy guidance. At the operational level, command-and-control structures serve as the critical interface between strategic intent and tactical execution. These entities are responsible for defining the technical and operational boundaries in which AWS may function, monitoring system behavior in real-time, and ensuring that the level of autonomy conferred does not exceed permissible legal and ethical thresholds. This includes maintaining continuous situational assessment, retaining the capacity to override or abort AWS actions when necessary, and ensuring that AWS remain fully interoperable with human decision-making processes[140]. Finally, at the tactical level, operators, whether deployed in the field or managing systems remotely, retain direct responsibility for real-time engagement decisions. Operating within the parameters established by higher command, their immediate oversight and context are indispensable[141]. They must possess both the authority and the technical capability to intervene promptly, including halting or redirecting AWS actions in response to evolving battlefield conditions, particularly when doubts arise regarding target legality or the proportionality of an attack.

By distributing MHC responsibilities across these levels, this approach rejects the notion that control can be centralized in a single role without compromising operational accountability.

[137] L. Campani Farias et al. (2025), *Human control, bias and risk: Mapping the discussions at the 2024 CCW/GGE on LAWS.*
[138] C. Miller et al. (2023), *Meaningful Human Control of AI-based Systems: Workshop Technical Evaluation Report, Thematic Perspectives and Associated Scenarios.*
[139] U.S. Department of Defense (2023), *DoD Directive 3000.09 – Autonomy in Weapon Systems.*
[140] V. Boulanin et al. (2017), *Mapping the Development of Autonomy in Weapon Systems.*
[141] I. Bode et al. (2023), *Loitering Munitions and Unpredictability: Autonomy in Weapon Systems and Challenges to Human Control.*

Instead, it conceptualizes MHC as a layered safeguard in which strategic, operational, and tactical actors exercise different yet complementary forms of control over AWS, thereby reinforcing both operational integrity and compliance with IHL. The "who" dimension of MHC is inherently linked to the questions of "over what", "when", and "how" control is exercised. At each level of command, distinct responsibilities are delineated, strategic actors define the scope and intent of the mission, command-and-control structures establish and enforce the operational parameters, and tactical operators ensure that critical functions are managed in accordance with legal and ethical requirements during use. Strategic approvals precede deployment, operational oversight is maintained throughout the mission, and post-deployment assessments contribute to the accountability framework. These processes are implemented through a combination of rules of engagement, technical safeguards, continuous situational monitoring, and the capacity to override or abort AWS functions when necessary.

The distributed model aligns with established accountability mechanisms in conventional military doctrine[142] while addressing the additional complexity introduced by AWS, which may undertake functions that traditionally require human judgment. It ensures that no single point of failure, whether human error or technological malfunction, results in a loss of lawful oversight. Embedding such a layered structure within MHC frameworks is therefore not merely a procedural safeguard, but a fundamental element of command responsibility. Under IHL, commanders remain responsible for the conduct of their subordinates, including operating and supervising AWS. Where the use of AWS results in unlawful harm, accountability, can, and should extend throughout the chain of command, provided that oversight responsibilities have been adequately defined and documented. This underscores that MHC must be substantive, informed, and enforceable at all command levels, rather than reduced to symbolic or nominal human involvement.

A real-world example that highlights the impact of MHC on military operations involved the deployment of loitering munitions, also known as "kamikaze drones", during the 2020 Nagorno-Karabakh conflict between Armenia and Azerbaijan[143]. These drones, which can hover and search for targets before committing to an attack, raised significant concerns regarding the level of human oversight in real-time combat decisions. During this conflict,

[142] C. Miller et al. (2023), *Meaningful Human Control of AI-based Systems: Workshop Technical Evaluation Report, Thematic Perspectives and Associated Scenarios.*
[143] S. Shaikh and W. Rumbaugh (2020), *The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense.*

Azerbaijan extensively used the Israeli-made Harop drone, which has autonomous capabilities allowing it to identify and strike targets independently[144]. While these systems are intended to reduce incidents of unintended civilian casualties by enhancing precision, the lack of sufficient human control has sometimes led to the opposite outcome. For instance, in October 2020, a strike believed to have been conducted by a drone hit a church in Shusha, damaging the structure and injuring civilians[145]. This incident highlighted the challenges of ensuring that AWS are used in strict compliance with IHL, particularly concerning the principles of distinction and proportionality. The aftermath of these incidents prompted discussions within international defense communities about the necessity of enhancing MHC frameworks to ensure that critical decisions, such as the identification and engagement of targets, involve substantial human judgment[146]. The debate continues over how to implement these controls without undermining the operational advantages of autonomous systems, underscoring the need for a balanced approach that safeguards both effectiveness and ethical standards in military operations.

The transparency of AWS operations, facilitated by MHC, is crucial for ensuring that military activities are visible and accountable to both the public and international regulatory bodies[147]. This transparency is essential for maintaining public trust and upholding IHL. The ICRC has played a crucial role in promoting transparency in military operations. It has consistently emphasized the need for clear operational visibility to ensure that AWS deployments comply with IHL[148]. This perspective underscores the importance of MHC in establishing an environment where AWS actions can be monitored and scrutinized by external entities, including international humanitarian organizations and civil society groups. The ICRC's advocacy underscores the importance of having robust mechanisms in place to review and regulate the use of AWS, confirming that such systems do not operate in a legal vacuum and that their deployment does not lead to unintended humanitarian consequences[149]. In a similar vein, the GGE on CCW outlines important guiding principles on *Emerging Technologies in the*

[144] I. Bode and T.F.A. Watts (2023), *Loitering Munitions and Unpredictability: Autonomy in Weapon Systems and Challenges to Human Control.*
[145] Human Rights Watch (2020), *Azerbaijan: Attack on Church Possible War Crime.*
[146] I. Bode and T.F.A. Watts (2023), *Loitering Munitions: Flagging an Urgent need for Legally Binding Rules for Autonomy in Weapon Systems.*
[147] C. Miller et al. (2023), *Meaningful Human Control of AI-based Systems: Workshop Technical Evaluation Report, Thematic Perspectives and Associated Scenarios.*
[148] N. Davidson (2018), *A Legal Perspective: Autonomous Weapon Systems under International Humanitarian Law*.
[149] A-M. Eklund (2020), *Meaningful Human Control of Autonomous Weapon Systems*.

Area of LAWS[150]. These principles focus on promoting transparency and accountability in the use of AWS, serving as a global framework for the responsible deployment of autonomous systems. They emphasize the need for states to maintain control over and oversight of AWS deployments, advocating for clear procedural guidelines that ensure AWS operations align with international legal standards, thereby reinforcing the role of MHC in maintaining oversight and accountability. By doing so, it ensures that every decision made by AWS is traceable and subject to human oversight, demonstrating that decisions are made with responsibility. Efforts to enhance transparency in AWS operations are directly linked to the broader goals of ensuring compliance with international norms and maintaining public confidence in military practices.

Building on the importance of transparency and public accountability, it is equally crucial to examine the internal mechanisms that support these principles. MHC plays a pivotal role in this context by clearly defining and enforcing the chain of responsibility within the deployment and operation of AWS[151]. This control mechanism is essential to ensure that every action taken by AWS is accountable and aligns with the established command structures, from the highest levels of military strategy down to tactical field operations. The implementation of MHC within AWS operations requires a clear definition of roles across all levels of command and control. This guarantees that from operational commanders to on-the-ground operators, everyone is fully aware of their responsibilities and the ethical implications of their decisions. For instance, commanders are responsible for the strategic deployment of AWS, while operators manage real-time tactical choices, ensuring that each level of operation adheres to strict guidelines and rules of engagement[152]. This structured approach helps prevent instances where the lack of oversight could lead to unauthorized or unintended use of military force. The critical need for robust MHC frameworks is underscored by the example previously discussed regarding the 2020 Nagorno-Karabakh conflict[153]. The deployment of loitering munitions, specifically the use of the Israeli-made Harop drone, demonstrated severe oversight challenges and the consequences of inadequate human control[154]. By referencing the structured implementation of MHC and linking it to specific examples of its impact, such as seen in Nagorno-Karabakh, the

[150] CCW (2019), *Guiding Principles Affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems.*
[151] J. Kwik (2022), *A Practicable Operationalization of Meaningful Human Control*.
[152] L. Trabucco (2023), *What Is Meaningful Human Control, Anyway? Cracking the Code on Autonomous Weapons and Human Judgment*.
[153] S. Shaikh and W. Rumbaugh (2020), *The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense.*
[154] I. Bode and T.F.A. Watts (2023), *Loitering Munitions and Unpredictability: Autonomy in Weapon Systems and Challenges to Human Control.*

necessity of establishing and adhering to well-defined roles within AWS operations becomes evident. Such adherence ensures that all military actions can be traced back to accountable individuals. This approach not only safeguards operational effectiveness but also ensures that military engagements are conducted within ethical and legal frameworks, reinforcing the legitimacy and accountability of using advanced technologies in modern warfare.

3.4. Concluding Remarks

This chapter has rigorously examined the essential elements of MHC in AWS, with a particular focus on context control, human supervision, and accountability. Throughout this discussion, the mechanisms by which MHC ensures that AWS operate within the bounds of ethical norms and IHL, as highlighted by the guidelines from the ICRC[155] and mandates such as Article 36 of the AP I to the Geneva Conventions[156]. This exploration has demonstrated that robust MHC mechanisms are not merely enhancements to AWS but rather foundational requirements for maintaining a chain of human responsibility and accountability. These mechanisms ensure that decisions within AWS are traceable and transparent, thereby preventing the erosion of ethical standards and reducing the risk of violations of IHL. By implementing robust supervision controls and comprehensive context analysis capabilities, MHC fosters a controlled operational environment where human judgment retains ultimate authority over critical military decisions. The practical examples discussed, including deployment scenarios in conflict zones such as Nagorno-Karabakh[157], illustrate the real-world implications of insufficient MHC. These examples have underscored the potential consequences of relinquishing control to AWS without adequate human oversight, leading to operational decisions that might escalate conflicts unpredictably and result in civilian casualties. Such outcomes demonstrate the necessity for MHC frameworks that integrate rigorous authorization protocols and real-time oversight capabilities, ensuring AWS actions align with established legal and ethical standards.

The analysis of the sub-question "*How does meaningful human control contribute to accountability in the deployment of AWS?"* demonstrates that MHC is indispensable. It ensures that clear and consistent accountability standards govern all actions taken by AWS. MHC

[155] ICRC (2022), *ICRC Position on Autonomous Weapon Systems*.
[156] V. Boulanin (2015), *Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems.*
[157] S. Shaikh and W. Rumbaugh (2020), *The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense.*

facilitates compliance with military directives and enhances public trust in military engagements, which is critical in maintaining operational legitimacy. As AWS are increasingly integrated into military operations, the role of MHC in establishing accountability remains crucial. It serves to protect both those on the battlefield and the ethical integrity of military strategy. The centralization of MHC in the design and deployment of AWS is therefore vital for preserving human accountability and upholding the high moral standards expected in contemporary military conduct. By concluding this chapter, the critical need for continued research and development in MHC frameworks is reaffirmed to enhance their efficacy and responsiveness to evolving technological landscapes. As progress is made, it remains imperative to commit to improving these controls, ensuring that AWS operations are not only practical but also ethically and legally defensible.

Conclusion – Moving Forward in the Pursuit of a Definition of MHC

At the intersection of technological innovation and ethical warfare, the rapid development of AWS presents unprecedented challenges to existing legal frameworks. This conclusion addresses a crucial sub-question of the thesis: *"What would a comprehensive legal framework for AWS look like, and how can it balance technological advances with human control?",* Through this exploration, it first proposes a clear and actionable definition of MHC. The analysis then engages with the existing CCW GGE rolling text[158], developed through consensus-based negotiations, to identify the modifications or additions required to produce a treaty capable of addressing the ethical, legal, and operational imperatives essential for both contemporary and future military technologies.

The need to define and regulate AWS under international law is driven by the urgent requirement to harness technological innovations for enhancing national and global security, while simultaneously ensuring these technologies adhere to the principles of ethical warfare and IHL. Drawing upon the authoritative recommendations of influential organizations such as the ICRC, Article 36, and the Campaign to Stop Killer Robots. Each of these entities advocates for stringent controls and the establishment of clear legal standards that ensure human oversight over AWS. In particular, this conclusion engages with the CCW GGE rolling text as the basis for adopting and operationalizing these definitions and principles within a global treaty framework. The analysis proposes targeted modifications and additions to integrate the critical

[158] CCW GGE on LAWS (2025), *Rolling text, status date: 12 May 2025.*

elements of MHC, thereby balancing the imperative for technological advancement with the necessity for ethical responsibility. This balance is crucial to ensure that AWS deployments enhance security without compromising human dignity or violating legal standards.

The conclusion will therefore begin by defining MHC through a precise and actionable definition that emphasizes transparency, accountability, and technical standards. It will then examine the structure and key provisions of the CCW GGE rolling text, assessing its current treatment of MHC and identifying targeted amendments to strengthen legal obligations, operational guidelines, compliance mechanisms, and support for innovation. Further discussions will explore how international bodies, most notably the CCW, can implement and enforce a revised text that balances technological innovation with ethical responsibility.
By engaging directly with this consensus-based framework, the conclusion seeks to demonstrate how carefully calibrated modifications can enhance its regulatory capacity. The objective is to ensure that international law remains adaptable and resilient, serving as a practical tool for managing the complexities and ethical dilemmas posed by these advancing technologies, while safeguarding humanity's interests and upholding the highest standards of international law. However, the effectiveness of such a framework is inextricably linked to the political, institutional, and geopolitical dynamics that will ultimately determine its adoption, implementation, and long-term enforceability.

4.1. Core Components of MHC: Transparency, Accountability, and Technical Standards

As established throughout this thesis, MHC is pivotal in the governance of AWS, ensuring that these technologies align with international law and the standards of ethical warfare. MHC mandates that substantial human judgment is central in guiding the deployment, operation, and engagement of AWS[159]. This control is essential to prevent unethical outcomes and safeguard human dignity, thereby reinforcing the principles outlined in earlier chapters. MHC is defined as the required degree of human judgment and intervention in the critical functions of selecting and engaging targets by AWS. This is essential to ensure that decisions made by these systems are both reversible and subject to human oversight. It requires that human operators are not

[159] H. Syse (2023), *Meaningful Human Control*

merely observers but active participants in the decision-making process concerning the life-or-death decisions executed by AWS[160].

The framework of MHC is built on three foundational pillars: Transparency, Accountability, and Technical Standards.

a. Transparency

Within the framework of MHC, transparency is not merely a procedural requirement but a foundational principle that ensures the ethical deployment and operation of AWS[161]. Transparency involves providing clear, comprehensible, and accessible information about the mechanisms by which AWS function and make decisions. This clarity is crucial for enabling effective human oversight and ensuring that these systems operate within established legal and ethical parameters. For AWS, transparency begins with the documentation of both the design and decision-making processes. This documentation must detail the algorithms and operational parameters under which AWS operate, including the data used for target recognition and engagement decisions. As explored in previous chapters, the complexity of machine learning models used in AWS can obscure the decision-making process, making it difficult for operators to understand or predict the system's actions without comprehensive documentation.

Transparency also necessitates AWS operations to be auditable. This means that every operation, an engagement, a disarmament, or a patrol, must be recorded in a manner that allows external reviewers, such as military auditors, legal experts, or international oversight bodies, to verify compliance with IHL and rules of engagement. The ability to audit these systems is essential, as it enables verification that AWS actions are consistent with their programming and the ethical guidelines set forth at the international level[162]. Moreover, the information provided must not only be accessible but also comprehensible to those responsible for overseeing these systems. This includes developing interfaces and reporting mechanisms that present data in a clear and accessible manner, enabling human operators to make informed decisions quickly and efficiently. Training for operators should include comprehensive education on how AWS

[160] A-M. Eklund (2020), *Meaningful Human Control of Autonomous Weapon Systems*,
[161] C, Miller et al. (2023), *Meaningful Human Control of AI-based Systems: Workshop Technical Evaluation Report, Thematic Perspectives and Associated Scenarios.*
[162] V. Boulanin et al. (2021), *Autonomous Weapon Systems and International Humanitarian Law: Identifying Limits and the Required Type and Degree of Human–Machine Interaction.*

process information and make decisions, enhancing transparency and reducing the 'black box' nature of advanced algorithms.

b. Accountability

Accountability within the framework of MHC is paramount, it ensures that every action executed by an AWS can be directly attributed to specific human operators or command decisions within the established military hierarchy. This traceability is critical for maintaining a clear line of command and responsibility, which is fundamental to both ethical military operations and compliance with IHL. Accountability requires well-defined protocols that unequivocally assign responsibility for the actions undertaken by AWS. These protocols must define who within the command chain is responsible at various stages of AWS operation – from deployment decisions to target engagements and post-engagement assessments[163]. Such protocols ensure that decisions made by AWS, guided by human operators or commanders, are in strict adherence to rules of engagement and the principles of IHL, as discussed in earlier chapters addressing the ethical implications of autonomous engagements.

Enhancing transparency, as highlighted earlier, is indispensable for achieving accountability. Comprehensive documentation of AWS operations allows for effective oversight and audits. This ensures that all actions are logged and traceable back to human decisions, which is essential for legal and ethical reviews as well as post-operation analysis. Documentation should include detailed logs of engagement decisions, sensor data interpretations, and the rationale behind each action, ensuring that these records are accessible for review by authorized personnel. The auditability of AWS ensure that stakeholders can trace any questionable actions back to specific decisions or system failures. This traceability is crucial not only for addressing individual incidents but also for identifying systemic issues that may require adjustments in AWS protocols or operational tactics. Regular audits and thorough post-mission analyses help pinpoint recurring errors and guide necessary modifications to deployment strategies and rules of engagement, thereby improving the overall reliability and ethical alignment of AWS operations.

[163] A. Seixas Nunes (2022), *Autonomous Weapons Systems and Deploying States. Making Designers and Programmers Accountable*.

c. Technical Standards

Technical standards form a cornerstone of MHC over AWS, establishing strict operational protocols that maintain human oversight and safeguard ethical engagements. These guidelines not only define the boundaries of AWS autonomy but also ensure that human operators retain ultimate control over critical military decisions, especially those that could have significant consequences. At the center of technical standards are protocols like HITL and HOTL[164]. HITL systems require human operators to initiate any critical action, particularly those involving target engagement, ensuring that each decision to use lethal force is made with direct human oversight. HOTL systems, while allowing AWS to operate autonomously within set parameters, still ensure that humans can intervene and override decisions at crucial moments. This level of human involvement is vital for maintaining accountability, particularly in complex and rapidly changing combat environments where ethical and legal judgments are paramount.

These standards impose specific constraints on the autonomy of AWS. These include limitations on the types of targets AWS can engage with, the conditions under which they can initiate engagements, and rules governing the use of force. For instance, AWS might be programmed to identify and engage only combatant targets in accordance with IHL, explicitly avoiding non-combatants or protected structures such as schools or hospitals. These constraints are crucial for preventing unlawful engagements and ensuring that operations adhere to the principles of distinction and proportionality mandated by international law. Before deployment, AWS are subjected to comprehensive testing to ensure compliance with all operational guidelines and ethical standards. This testing phase assesses the system's ability to accurately identify targets, evaluate its decision-making algorithms, and verify its adherence to the rules of engagement under various scenarios[165]. Rigorous testing helps identify potential flaws in system design or function that could lead to unintended or unethical actions, allowing for corrections before operational deployment.

Additionally, technical standards require the integration of fail-safe mechanisms that can interrupt or reverse AWS operations if they deviate from expected behaviors[166]. These might include emergency shutdown systems or software that can detect and rectify malfunctions,

[164] P. Scharre (2016), *Autonomous Weapons and Operational Risk.*
[165] Ibid.
[166] D. Amoroso and G. Tamburrini (2021), *Toward a Normative Model of Meaningful Human Control Over Weapons Systems*.

software that can respond to situations escalating beyond predicted parameters. Given the rapid pace of technological advancement, technical standards also require AWS to be adaptable to new threats and scenarios. This means that systems must be capable of receiving updates and modifications that enhance their ethical and legal compliance over time without requiring complete redesigns. This adaptability is essential for ensuring that AWS remain effective and compliant with international law as new moral dilemmas and technological capabilities merge.

Integrating MHC into the operational practice of AWS involves embedding the principles of transparency, accountability, and technical standards directly into the daily operations and management of these systems. This integration ensures that MHC is more than a theoretical framework, it constitutes a practical and operational dimension of military engagement with AWS. It entails the establishment of clear protocols for human oversight and decision-making, continuous monitoring of system performance, and the regular updating of operational guidelines to adapt to new challenges and technological advancements. This preliminary integration lays the groundwork for a more comprehensive examination of how international bodies and military organizations can effectively implement, manage, and refine these practices to ensure ethical compliance and operational effectiveness in rapidly evolving combat environments. Building on the foundational elements of MHC, the next section of this conclusion turns to the Rolling Text of the CCW GGE. It will examine how these principles can be translated into a binding framework, demonstrating how MHC operates as the baseline standard to ensure that AWS function within strict legal and ethical parameters.

4.2. Refining the CCW GGE Rolling Text through the Lens of MHC

This section undertakes a direct engagement with the Rolling Text adopted by the GGE under the CCW on the 12th May 2025[167]. As the most advanced consensus-oriented framework currently under negotiation regulating of LAWS, the Rolling Text presents a significant point of reference for assessing how far the existing treaty practice is capable of addressing the regulatory challenges posed by emerging autonomous military technologies. As a product of multilateral deliberation, it affirms the applicability of IHL and introduces prohibitions, precautionary measures, and lifecycle-oriented safeguards. At the same time, it leaves unresolved critical questions regarding the definition, scope, and operationalization of human

[167] CCW GGE on LAWS (2025), *Rolling text, status date: 12 May 2025.*

control, particularly concerning accountability, reliability, and the consistent application of IHL in complex operational contexts. Building on the conceptual foundations and lifecycle safeguards developed in the preceding chapters, this section identifies amendments and supplementary provisions designed to refine the Rolling Text, transforming it from an aspirational guidance to a framework of enforceable legal obligations.

The objective is to recalibrate the Rolling Text into a treaty-capable framework anchored in the principles of MHC. The forthcoming subsections demonstrate how definitional clarity, binding safeguards, enforceable governance, international oversight, and provisions for responsible innovation collectively embed transparency, accountability, and technical standards across the entire lifecycle of AWS.

4.2.1. Overview of the CCW GGE Rolling Text

The Rolling Text is structured into five principal sections. The first defines LAWS as systems capable of selecting and engaging targets without human intervention in the execution of these functions, though this definition is explicitly provisional and with prejudice to future refinements. The second section reaffirms the continued applicability of IHL to all weapons, past, present, or future. It refers to the Marten Clause and emphasizes the necessity of context-appropriate human judgment and control to ensure compliance with the principles of distinction, proportionality, and precautions in attack. The third section prohibits indiscriminate systems that cause superfluous injury or unnecessary suffering, target civilians or civilian objects, or whose effects cannot be anticipated or controlled. It further enumerates risk-mitigation measures, including predictability, traceability, the maintenance of a responsible chain of command, restrictions on parameters and learning functions, and mechanisms for deactivation or self-neutralization. The fourth section addresses lifecycle-related measures, recommending legal reviews, realistic testing, bias mitigation, and training, while also encouraging states not to develop, produce, or transfer systems incapable of complying with IHL. The fifth and final section affirms that responsibility lies with states and individuals rather than machines, calling for adaptations to training protocols, rules of engagement, and domestic mechanisms of investigation and redress.

Considered in its entirety, the Rolling Text constitutes a meaningful step toward embedding LAWS within the normative framework of IHL, prohibiting inherently unlawful systems, and

outlining preliminary safeguards for risk mitigation and lifecycle governance. Nevertheless, its normative structure remains underdeveloped. The concept of human judgment and control, although referenced throughout, is left undefined, core obligations are formulated in discretionary rather than mandatory terms, and the framework omits institutional mechanisms for international oversight and structured transparency. For the Rolling Text to serve as a credible foundation for a legally binding instrument, its indeterminate reference to human control must be translated into a concrete and enforceable standard. The conception of MHC developed in the preceding chapters, defined through the interrelated pillars of transparency, accountability, and technical safeguards, provides a coherent and operationalizable framework for this purpose.

4.2.2. From Indeterminate "Human Judgment" to a Codified Standard of Control

The Rolling Text refers to "context-appropriate human judgment and control" as a condition for the lawful deployment of AWS, yet it fails to provide a definition or to specify how this standard should be operationalized across the design, testing, deployment, and engagement phases. This conceptual indeterminacy permits divergent state interpretations, thereby undermining legal certainty, the consistent application of IHL, and the attribution of responsibility within established accountability frameworks.[168] For the regulatory framework to acquire binding legal force, the notion of human control must be articulated as a justiciable standard, capable of consistent interpretation and application by states, judicial bodies, and international oversight mechanisms. The conception of MHC developed in the preceding chapters offers a concrete and legally operable standard. MHC requires that human operators retain effective oversight and ultimate responsibility for all critical functions of AWS. It is grounded in three interdependent pillars, transparency, accountability, and technical safeguards, which together ensure that control is auditable, attributable, and enforceable throughout the entire system lifecycle.

To operationalize this requirement, the Rolling Text should be amended to incorporate a definitional clause codifying MHC as the foundational standard. For instance:

[168] G. Sheehan (2025), *Cheap Drones, Expensive Lessons: Ethics, Innovation, and Regulation of Autonomous Weapons Systems.*

"*Meaningful Human Control (MHC) refers to the essential standards and practices established to ensure human beings maintain effective oversight and ultimate responsibility for decisions made by AWS. MHC is characterized by three core elements designed to ensure that AWS operations are aligned with ethical norms, legal standards, and strategic directives:*

- *Transparency: MHC mandates comprehensive transparency in AWS operations. This includes clear documentation of the decision-making algorithms, operational parameters, and the logic behind target engagements. Transparency is crucial for enabling effective oversight, ensuring ethical accountability, and ensuring compliance with international law.*

- *Accountability: Under MHC, all actions taken by AWS must be attributable to human operators, who are accountable for those actions. This requires well-defined command-and-control protocols that trace all decisions back to identifiable individuals within a command structure.*

- *Technical Standards: MHC includes strict technical standards that define and limit the autonomy of AWS to ensure continuous human control, such as safety and reliability protocols and fail-safe mechanisms.* "

By codifying MHC as the legal baseline, the framework would transform the Rolling Text's indeterminate reference to human judgment into a concrete and enforceable obligation. This incorporation would promote consistent interpretation and application across jurisdictions, strengthen compliance mechanisms, and anchor accountability at both state and individual levels, thereby aligning the trajectory of technological development with the normative imperatives of IHL and ethical responsibility.

4.2.3. Embedding Binding Safeguards and Contextual Constraints

Section III of the Rolling Text appropriately prohibits indiscriminate systems and those whose effects cannot be anticipated or controlled, and identifies risk-mitigation measures, including predictability, traceability, and command responsibility. However, these provisions remain expressed in discretionary terms and fail to impose concrete restrictions on the operational contexts in which autonomy may be deployed. To ensure compatibility with IHL, these

measures must be reformulated as binding obligations explicitly anchored to the principle of MHC.

Within this standard, human supervision must go through clearly defined modalities of control. HITL configurations are imperative for any AWS employing lethal force, ensuring that human operators initiate and authorize every critical engagement, thereby embedding ethical and legal judgment into the decision-making process. HOTL oversight may be acceptable for systems operating autonomously within strictly defined parameters, provided that operators retain continuous situational awareness and the immediate capacity to intervene, alter, or terminate the system's activity. This distinction reflects a graduated safeguard approach, the higher the humanitarian risks, the more stringent the requirement for direct human involvement[169].

Context-specific constraints must further prohibit the autonomous engagement of targets by AWS in operational environments where adherence to the principle of distinction cannot be reliably ensured, such as densely populated areas or in proximity to protected sites, including hospitals, schools, and cultural property. In such contexts, the application of HITL configurations constitutes an essential safeguard, guaranteeing that lethal decisions remain subject to direct human judgment. Additionally, AWS deployed in legally or operationally ambiguous scenarios must be equipped with programmed safeguards capable of automatically suspending autonomous functions in response to operational uncertainty, thereby preventing the delegation of lethal decision-making to algorithms in situations where the risk of civilian harm cannot be effectively mitigated.

Effective accountability further necessitates the generation of auditable records for each AWS deployment. Secure logging of sensor inputs, algorithmic outputs, human interventions, and final engagement decisions must be mandated to create a verifiable documentary record.[170] These records serve as the foundation for attributing responsibility within the command structure and enable both domestic and international oversight mechanisms to evaluate compliance with IHL and the standards of MHC. In the absence of such verifiable data, accountability risks becoming abstract and ineffectual, thereby undermining both the pursuit of justice for victims and the credibility of compliance mechanisms.

[169] P. Scharre (2016), *Autonomous Weapons and Operational Risk*, Center for a New American Security.
[170] V. Boulanin, et al. (2020), *Responsible Artificial Intelligence Research and Innovation for International Peace and Security.*

In addition, AWS must be equipped with embedded technical safeguards that ensure adherence to IHL and MHC. These include constraints that limit targeting to lawful military objectives, establish exclusion zones around protected persons and objects, and incorporate fail-safe functionalities capable of immediate deactivation in the event of malfunction, the unexpected presence of civilians, or loss of communication. In parallel, states must ensure that all individuals involved in the operation and oversight of AWS undergo specialized training that encompasses both system functionalities and the legal and ethical constraints governing their use[171]. Only adequately trained operators, capable of interpreting, supervising, and intervening in AWS operations in real-time, can ensure that human judgment remains the decisive factor.

By elevating these measures from recommended best practices to binding treaty obligations, the revised framework would replace discretionary safeguards with enforceable standards, thereby ensuring that the deployment and use of AWS remain subject to consistent legal and ethical constraints.

4.2.4. Enforcing Lifecycle Governance

Section IV from the Rolling Text identifies legal reviews, realistic testing, and bias mitigation as essential safeguards for the deployment of AWS. However, the absence of requirements for institutional independence, mandatory re-evaluation following system modifications, and transparency obligations extending beyond the national level significantly weakens the credibility of lifecycle governance. To ensure that AWS remain legally compliant and ethically defensible throughout their operational existence, such safeguards must be formalized as binding obligations firmly grounded in the standard of MHC.

Legal reviews must be conducted not only before the development, acquisition, or deployment of any AWS, but also whenever significant modifications affect targeting logic or operational performance, including software updates, model retraining, or changes to sensor configurations[172]. This requirement reflects the preventive rationale of Article 36 of AP I[173], ensuring that compliance with IHL and international human rights norms is continuously verified throughout a system's evolution. These assessments shall be carried out by

[171] ICRC (2022), *ICRC Position on Autonomous Weapon Systems*.
[172] V. Boulanin (2015), *Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems.*
[173] R. Moyes (2016), *Key Elements of Meaningful Human Control*.

institutionally independent panels composed of multidisciplinary expertise, including specialists in IHL, human rights, military operators, system engineers, and ethicists. Where appropriate, civil society participation may reinforce the legitimacy and inclusiveness of the process. Such panels must apply transparent, evidence-based criteria and explicitly integrate MHC as the central evaluative standard, assessing whether human judgment remains the decisive factor in target selection, engagement decisions, and mission termination. In this regard, the legal guidance developed by the ICRC on Article 36 reviews offers practical methodologies and interpretive benchmarks for the assessment of emerging technologies, helping to ensure that AWS are evaluated in accordance with IHL and broader humanitarian standards.

States must retain review documentation, testing results, operational constraints, and legal assessments in secure and auditable formats. Summaries must be submitted to the international oversight authority upon request, ensuring both transparency and harmonized interpretation across jurisdictions. AWS that fail legal review must be immediately suspended, and systems that cannot be rendered compliant must be permanently withdrawn from service. Repeated failures or intentional non-submission would constitute a material breach of treaty obligations, activating enforcement procedures as defined in section 4.2.5. This approach aligns with established arms control regimes, where reporting and compliance operate as mandatory legal obligations rather than discretionary practices.

Operational testing must be conducted under realistic, diverse, and stress-tested conditions to reveal hidden vulnerabilities and assess reliability under unpredictable battlefield circumstances[174]. States must systematically identify and mitigate sources of bias, whether within datasets, models, or operator decision-making processes, and document corrective actions accordingly. Review mechanisms must confirm that AWS operations comply with IHL principles and do not result in discriminatory or disproportionate effects. These evaluations must remain iterative, legal and technical reviews are to be repeated whenever upgrades, retraining, or operational experience reveal emergent risks. AWS interfaces must remain interpretable and operator-oriented, enabling human supervisors to understand system behavior and intervene in real-time. Transparency further requires the inclusion of test results, review outcomes, and mitigation strategies in periodic reports submitted to the international oversight

[174] D.Copeland, et al. (2022), *The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems*.

authority. This prevents unilateral determinations of adequacy, promotes accountability, and fosters the development of harmonized global standards.

Reformulating Section IV along with these observations, lifecycle governance is transformed from an aspirational recommendation into a binding treaty obligation, directly linked to the implementation of MHC. Legal reviews, realistic testing, and bias mitigation become continuous, transparent, and independently verifiable safeguards. In doing so, lifecycle governance is embedded as a structural guarantee, ensuring that AWS remain lawful by design and throughout deployment, thereby bridging the gap between normative ambitions and enforceable legal commitment. Moreover, MHC must not be conceived as a static benchmark or a one-time certification event, rather, it constitutes a dynamic and evolving standard. Lifecycle governance must therefore function as a continuous process of legal, technical, and ethical recalibration, ensuring that human oversight and legal compliance are sustained throughout the AWS lifecycle as operational contexts and technologies evolve.

4.2.5. Addressing the Enforcement Gap through Transparency, Oversight, and Compliance Mechanisms

Section V of the Rolling Text assigns responsibility for AWS use to states and individuals, encouraging the establishment of domestic mechanisms of investigation and redress. While these elements are necessary, they remain insufficient in the absence of robust international oversight. Without structured transparency and external supervision, compliance with IHL and MHC-aligned obligations risks remaining unverifiable, unevenly implemented, and vulnerable to selective interpretation, thereby generating a fragmented accountability landscape. To ensure that obligations are uniformly upheld and enforcement is credible, Section V must be supplemented with binding provisions establishing international oversight, procedural transparency, and enforceable compliance mechanisms.

A dedicated international supervisory authority[175] must be established to monitor and ensure adherence to the obligations grounded in the standard of MHC. This authority operates independently under the auspices of the UN or an equivalent multilateral framework, this body must possess multidisciplinary expertise in IHL, military affairs, AI, ethics, and civilian

[175] While the notion of international oversight has been broadly advocated by civil society actors and academic scholars, the establishment of a dedicated international supervisory authority has not yet been formally advanced within the existing regulatory discourse.

protection. Its core functions include receiving and reviewing annual transparency reports from states parties, conducting document-based assessments, and, where applicable, on-site audits, either upon state consent or in response to predefined procedural conditions, administering a peer-review mechanism among states parties to promote harmonization of standards in a non-politicized manner, and publishing public implementation reports with appropriate safeguards for sensitive or classified information. These functions are essential to promoting global confidence and legal consistency. Based on credible and substantiated indications of a potential breach, the international supervisory authority is empowered to initiate a formal fact-finding inquiry, including access to operational records, legal assessments, and system logs. Where appropriate, matters may be referred to competent international institutions, including the UN Security Council or the International Criminal Court, depending on the gravity of the breach. The enforcement mechanism shall be structured around a graduated response model, prioritizing remediation and reintegration over purely punitive measures. Available responses include publishing non-compliance notifications, temporary suspension from AWS-related cooperation frameworks, recommendations for limiting access to dual-use technologies, and, where proportionate, financial or diplomatic consequences. These mechanisms aim to deter systematic non-compliance while allowing pathways for corrective action and reintegration into the treaty framework.

In alignment with the principles of transparency and accountability underpinning MHC, the supervisory authority must establish formal channels for civil society and research institutions to submit relevant information and evaluations. Regular multistakeholder forums, bringing together state representatives, technical experts, and advocacy groups such as the Campaign to Stop Killer Robots, are institutionalized to promote best practices and address emerging risks. Additionally, the authority also publishes aggregate trend analyses drawn from compliance data and incident reports, contributing to cross-jurisdictional learning and the progressive development of normative standards.

By institutionalizing these mechanisms, the proposed amendment transforms accountability from a purely domestic obligation to an internationally verifiable regime. While national procedures remain the first layer of responsibility, their effectiveness is reinforced by structured transparency, external review, international supervision, and corrective compliance mechanisms. This dual-layered approach preserves the intergovernmental character of the CCW while embedding MHC into the structural logic of treaty enforcement.

4.2.6. Safeguarding Responsible Innovation within the Framework of MHC

While most of the Rolling Text and the proposed amendments primarily address prohibitions, safeguards, and compliance mechanisms, a comprehensive regulatory framework must also provide for the facilitation of responsible innovation[176]. States are unlikely to endorse an instrument perceived as impeding technological advancement or disregarding legitimate defense imperatives. To ensure sustained engagement and broad adherence, the treaty architecture must demonstrate that the development of merging technologies and the normative demands of MHC can operate in harmony rather than in opposition.

In this context, states parties may be permitted to operate strictly regulated experimental environments for the research and testing of AWS, subject to rigorous HITL or HOTL protocols, independent supervisory oversight, and mandatory logging of all trial data. The safeguards ensure that innovation remains subject to ethical scrutiny and human control. The transition from experimentation to operational status must be contingent upon demonstrable compliance with the constitutive elements of MHC, including transparency, accountability, and technical safeguards, thereby establishing certification as a precondition for deployment and a regulatory interface between innovation and legal obligation[177]. To prevent fragmented regulatory practices and enhance interoperability, state parties must engage in international cooperation on technical standards, audit methodologies, and data-logging formats. Such collaboration enables robust oversight while maintaining protection for sensitive or classified system architectures. In recognition of the dual-use nature of many AI technologies, the treaty must also mandate the adoption of control mechanisms that mitigate the risk of diversion or misuse. These include risk management protocols, benchmarks for bias detection and correction, and interpretability standards to prevent unlawful or indiscriminate applications.

By integrating responsible innovation within the treaty framework, the treaty avoids establishing a dichotomy between humanitarian restraint and technological progress. Instead, it advances an adaptive, learning-oriented governance model in which technological development is continually aligned with the ethical and legal imperatives of MHC and IHL. Accordingly, innovation is not constrained but directed towards the reinforcement of compliance, accountability, and human oversight throughout the lifecycle of AWS.

[176] V. Boulanin, et al. (2020), *Responsible Artificial Intelligence Research and Innovation for International Peace and Security.*
[177] A. Blanchard et al. (2024), *A Risk-Based Regulatory Approach to Autonomous Weapon Systems*.

4.2.7. A Calibrated Path Forward for the CCW

In this light, the Rolling Text needs to remain a static expression of political compromise. Its architecture, however provisional, already reflects the contours of a future treaty regime. With focused legal refinement, the framework can evolve into an instrument that not only affirms the centrality of human judgment in warfare but also embeds compliance, transparency, and accountability as enforceable obligations. Anchored in the principles of MHC, such a transformation would ensure that autonomy in AWS is regulated not merely through normative aspiration, but through binding international law. What remains is not a conceptual void, but the political will to translate consensus into codification, aligning governance with the ethical imperatives of our time and the legal standards that must guide the technologies of tomorrow.

4.3. From Norms to Practice: Navigating the Political Realities of Treaty Operationalization

The implementation of a legally binding framework on AWS, grounded in the principle of MHC, raises not only complex technical and legal questions but also substantial political, institutional, and geopolitical realities. As outlined in the preceding chapters, the normative framework basis for such regulations is well established in IHL, particularly through the principles of distinction, proportionality, and military necessity. However, translating these principles into enforceable treaty obligations is far from straightforward. It requires more than legal drafting, it depends on sustained international coordination, the willingness of states to accept limitations on strategic autonomy, and the broader political economy of military innovation, which often prioritizes competitive advantage over collective ethical responsibility[178]. The gap between legal commitments and real-world enforcement is therefore not merely procedural but deeply embedded in the structural dynamics of global power and technology.

Efforts to regulate AWS face the structural tension between the imperatives of national sovereignty and the pursuit of collective ethical responsibility under IHL. Although many states publicly support the principles of IHL in armed conflict, they often resist binding legal instruments that could restrict their strategic freedom and technological autonomy. This is

[178] F. Sauer (2021), *Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible.*

particularly evident in discussions within the GGE operating the framework of the CCW, where exchanges on AWS have been ongoing for nearly a decade without leading to any binding agreement[179]. The result has been a series of non-binding guiding principles, valid for dialogue but insufficient to ensure compliance or prevent misuse.

This persistence of legal and political inertia is further complicated by the accelerated evolution of dual-use technologies, such as AI, machine learning, and sensor systems, which are designed for both civilian and military purposes. As addressed in earlier chapters, this fusion creates significant regulatory ambiguity, technologies initially developed for commercial or industrial applications can be rapidly adapted for military use, often outside the scope of conventional arms control frameworks[180]. Moreover, private sector entities, which increasingly lead innovation in AI and robotics, operate beyond the bounds of direct state control and often lie outside the jurisdiction of international humanitarian mechanisms. This fragmentation of authority not only weakens enforcement but also undermines transparency and ethical oversight in the development process. Furthermore, the global asymmetry in technological capabilities exacerbates regulatory fragmentation. States with advanced military-industrial infrastructures may perceive international regulation as a constraint on their competitive edge, particularly in contexts where strategic dominance is closely tied to emerging technologies. In contrast, states with fewer resources or less-developed technological capacity are more likely to view binding norms as a necessary safeguard against unchecked innovation. These divergent interests have led to a normative stagnation in international negotiations, where humanitarian concerns frequently come into tension with realpolitik and geopolitical calculations. Consequently, achieving consensus on adequate legal limits for AWS remains a complex challenge, driven as much by geopolitical interests and power dynamics as by international legal principles.

Despite these structural limitations, several existing international and regional institutions offer potential entry points for the partial implementation and oversight of the proposed treaty. In particular, the CCW GGE has made notable progress in recent months, culminating in the adoption of the Rolling Text in May 2025. Although not legally binding, this marks the most advanced consensus-oriented framework currently under negotiation for the regulation of AWS. As such, it could therefore serve as a foundational platform for fostering broader consensus, even if progress unfolds only through phased negotiations or structured discussions. The

[179] J. Dawes (2021), *UN Fails to Agree on 'Killer Robot' Ban as Nations Pour Billions Into Autonomous Weapons Research.*
[180] K. Harris (2023), *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*.

UNDOA[181], along with regional political or defense alliances, may also contribute to this trajectory by facilitating expert consultations, coordinating technical assistance, and supporting capacity-building for treaty implementation, particularly in states with limited regulatory frameworks or technological capabilities.

As outlined in subsection 4.2.5. of the refined framework, the creation of an independent international supervisory authority would further strengthen treaty implementation by institutionalizing a structured peer-review mechanism. This oversight model, inspired by existing human rights treaty bodies, would enable states to evaluate each other's compliance efforts in a depoliticized and reciprocal format. Far from challenging national sovereignty, this function is designed to enhance transparency, foster mutual accountability, and reinforce the legitimacy of legal reviews and operational protocols. Through regular documentation exchanges, on-site audits, and the publication of compliance reports, such a body could help operationalize the treaty's requirements in practice while preserving the procedural flexibility necessary to accommodate diverse national legal systems. Moreover, as discussed in subsection 4.2.4., existing structures such as Article 36 review bodies, required under AP I to the Geneva Conventions, already perform essential legal assessments of new weapons, means, and methods of warfare[182]. Drawing on ICRC legal guidance, these domestic institutions could play a pivotal role in contextualizing and applying MHC standards within national legal frameworks, thereby contributing to a harmonized baseline of ethical and legal conformity across jurisdictions. Considered as a whole, these institutional mechanisms demonstrate that, although global consensus remains elusive, the infrastructure for treaty operationalization is not absent. These mechanisms, though presently fragmented, could, if systematically integrated, establish a functional architecture for compliance monitoring and normative coherence.

Although the refined framework avoids speculative technical predictions, it affirms that MHC must not be conceived as a fixed benchmark or a one-time certification event. Instead, it constitutes a dynamic and evolving standard, requiring continuous legal, operational, and ethical oversight, especially as AWS are integrated into increasingly complex and unpredictable combat environments. As emphasized in subsection 4.2.4. and reflected in the CCW GGE

[181] UN (UNDOA), *Meetings of the Group of Governmental Experts* https://disarmament.unoda.org/meetings-of-the-group-of-governmental-experts/

[182] D. Copeland et al. (2022), *The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems*

Rolling Text, the obligation to conduct iterative legal reviews across all phases of the AWS lifecycle, design, testing, deployment, and field adaptation, is critical to ensuring sustained compliance with IHL and MHC principles[183]. Such reviews cannot be reduced to formalities, they must evolve alongside technological advancements and shifting battlefield realities. Equally important are the refined framework's transparency mechanisms, which aim to bridge the gap between legal enforceability and normative pressure. As previously examined, reporting obligations, including the documentation of engagement decisions, technical evaluations, and legal assessments, play a dual role. Legally, they provide the factual basis for monitoring and compliance. Politically, they function as soft enforcement tools, generating reputational incentives through the publication of best practices, expert scrutiny, and international visibility. These practices contribute to building a culture of accountability, whereby even powerful or reluctant actors may be indirectly pressured to align with established norms due to fear of reputational harm, diplomatic isolation, or public criticism. However, as the thesis has brought to light, such mechanisms remain inherently fragile. States with significant military-industrial capabilities and the political weight to resist international scrutiny are often the least likely to subject themselves to meaningful oversight. Their strategic interest in retaining autonomy over AWS development may override normative appeals, regardless of how well-grounded they are in law or ethics[184].

Ultimately, while the refined framework articulates a comprehensive and forward-looking legal framework for embedding MHC in AWS governance, its practical implementation depends on factors that extend beyond the realm of law alone. Asymmetries in power and technological development, divergent national security doctrines, and conflicting normative commitments will continue to define the international landscape in which this treaty would operate. This gap between legal idealism and political realism must be explicitly acknowledged, not as a weakness of the regulatory framework, but as an unavoidable condition of contemporary international lawmaking. Only by confronting these tensions openly can the treaty aspire to both legitimacy and durability in a global order shaped as much by political and economic forces as by humanitarian principles.

[183] D. Amoroso and G. Tamburrini (2021), *Toward a Normative Model of Meaningful Human Control Over Weapons Systems*.
[184] F. Sauer (2021), *Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible.*

4.4. Concluding Remarks

This thesis has unpacked the evolving notion of MHC in the regulation of AWS, examining how this concept may be defined with analytical precision and operationalized through legal and institutional frameworks to ensure compliance with IHL. The research addressed a central challenge, the absence of a universally accepted definition of MHC has left a critical regulatory gap in the governance of AWS. This is a gap that must be bridged if accountability, legality, and ethical legitimacy are to be preserved in a technologically mediated warfare.

A principal finding of this thesis is the articulation of MHC as a structured regulatory standard consisting of three independent pillars: transparency, accountability, and technical standards. Together, these components establish the substantive threshold required for human control to be considered legally operative and ethically legitimate under IHL. In this framework, MHC is understood as the preservation of informed, context-specific, and legally traceable human judgment over decisions involving the use of force by AWS. Human operators retain both the legal authority and the practical capacity to initiate, supervise, and, where necessary, override AWS functions. Moreover, such human intervention must be embedded within an institutional and procedural architecture that enables prior legal review and subsequent accountability, thereby ensuring that AWS conduct remains subject to IHL constraints throughout the entire decision-making process. The thesis further demonstrated that MHC must be operationalized as a continuous requirement embedded across the entire lifecycle of AWS, from system design and iterative legal reviews under Article 36 of AP I, to real-time deployment and post-engagement evaluation. MHC cannot be reduced to a symbolic presence or limited to retrospective accountability, instead, it must be operationalized through a combination of procedural safeguards and technical architectures. These include context-specific rules of engagement, HITL or HOTL mechanisms, robust fail-safes, and post-use audit records. Together, these safeguards ensure that AWS operations remain anchored in human agency and capable of upholding the fundamental principles of distinction, proportionality, and military necessity. MHC, in this sense, entails the legal possibility of human intervention, as well as the institutional capacity and operational clarity required to exercise such judgment at all critical points of decision-making in AWS activity.

Another core finding concerns the distributed nature of human control. MHC must be exercised through a layered structure of responsibility across strategic, operational, and tactical levels. This layered distribution reinforces the principle of command responsibility and ensures traceability within increasingly complex decision-making structures. By conceptualizing MHC as an integrated function of military doctrine rather than a static condition, the thesis highlights the institutional reforms necessary to preserve lawful oversight in the deployment of autonomous capabilities. Crucially, the thesis also underscores that the implementation of MHC is not solely a legal or technical issue, it is a political and institutional one. Despite a growing normative consensus on the necessity of human control, the translation of this principle into binding legal obligations remains hindered by divergent strategic interests, technological asymmetries, and geopolitical rivalries. As demonstrated in the analysis of the CCW GGE discussions and the proposal refinement of the Rolling Text, institutional stagnation and sovereign reticence to constrain strategic autonomy have significantly impeded meaningful progress. In this context, transparency mechanisms, such as peer-review procedures, reporting obligations, and the establishment of an international oversight body, emerge as critical instruments for bridging the gap between normative commitments and legal enforceability.

Ultimately, this thesis argues that operationalizing MHC is indispensable for the future governance of AWS. As technological systems increasingly shape life-and-death decisions, the legal and ethical imperative to ensure that such decisions remain within the domain of human judgment is a foundational condition of lawful warfare. While the implementation of MHC will require robust treaty commitments, institutional mechanisms, and sustained political will, its core purpose remains clear: to safeguard the irreducible role of human responsibility in the conduct of hostilities, and to ensure that the advancement of autonomy in warfare does not erode the fundamental protections enshrined in IHL.

BIBLIOGRAPHY

1. Afonso Seixas Nunes, *Autonomous Weapons Systems and Deploying States. Making Designers and Programmers Accountable*, University of Saint Louis, May 4, 2022. https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD161/NeDef161_4_AfonsoSeixasNunes.pdf
2. Alexander Blanchard, Claudio Novelli, Luciano Floridi and Mariarosaria Taddeo, *A Risk-Based Regulatory Approach to Autonomous Weapon Systems*, April 2024. https://core.ac.uk/download/603657337.pdf
3. Amanda Musco Eklund, *Meaningful Human Control of Autonomous Weapon Systems*, FOI Defence Research Agency, February 2020. https://www.fcas-forum.eu/publications/Meaningful-Human-Control-of-Autonomous-Weapon-Systems-Eklund.pdf
4. Anna-Katharina Ferl, *Imagining Meaningful Human Control: Autonomous Weapons and the (De-) Legitimisation of Future Warfare*, Global Society, July 9, 2023. https://doi.org/10.1080/13600826.2023.2233004
5. Article 36, *Killer Robots: UK Government Policy on Fully Autonomous Weapons*, April 2013. https://article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf
6. Arun Rath, Raney Aronson-Rath, *Rules of Engagement*, FRONTLINE, February 7 and 19, 2012. https://www.pbs.org/wgbh/frontline/documentary/haditha/
7. Brooke Becher, *Brain Computer Interfaces (BCI), explained*, Builtin, June 12, 2025. https://builtin.com/hardware/brain-computer-interface-bci
8. Luis Campani Farias, Ana Beatriz T.D. Duarte, Manuela Le-Fort Magalhães, *Human control, bias and risk: Mapping the discussions at the 2024 CCW/GGE on LAWS,* The InterAgency, April 20, 2025. https://zenodo.org/records/15257771
9. CCW GGE on LAWS, *Report of the 2019 session of the GGE on Emerging Technologies in the Area of AWS,* CCW/GGE.1/2019/3, Geneva, March 25-29 and August 20-21, 2019. https://documents.unoda.org/wp-content/uploads/2020/09/CCW_GGE.1_2019_3_E.pdf
10. CCW GGE on LAWS, *Examples of existing CCW Protocols*, CCW/GGE.1/2024/CRP.2, Geneva, March 4-8 and August 26-30, 2024. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2024)/CCW_GGE1_2024_CRP.2.pdf

11. CCW GGE on LAWS, *Existing IHL applicable on LAWS,* CCW/GGE.1/2024/CRP.3, March 4-8 and August 26-30, 2024. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2024)/CCW_GGE1_2024_CRP.3.pdf
12. CCW, *Guiding Principles Affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems,* CCW/MSP/2019/9, December 13, 2019. https://www.ccdcoe.org/uploads/2020/02/UN-191213_CCW-MSP-Final-report-Annex-III_Guiding-Principles-affirmed-by-GGE.pdf
13. CCW GGE on LAWS, *Measures needed to ensure compliance with IHL and the identification of potential additional measures,* CCW/GGE.1/2024/CRP.4, March 4-8 and August 26-30, 2024. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2024)/CCW_GGE1_2024_CRP.4.pdf
14. CCW GGE on LAWS, *Rolling text, status date: 12 May 2025,* UN Office for Disarmament Affairs, May 12, 2025. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2025)/CCW_GGE_LAWS_-_Revised_rolling_text_as_of_12_May_2025.pdf
15. Chair's Summary, *Humanity at the Crossroads: Autonomous Weapon Systems and the Challenge of Regulation,* Vienna, April 30, 2024. https://www.bmeia.gv.at/fileadmin/user_upload/Zentrale/Aussenpolitik/Abruestung/AWS_2024/Chair_s_Summary.pdf
16. Charles P. Trumbull, *Autonomous Weapons: How Existing Law Can Regulate Future Weapons,* SSRN Electronic Journal, January 1, 2019. https://doi.org/10.2139/ssrn.3440981
17. Christian Chow, *Deep Learning for Aircraft Recognition Part I: Building a Convolutional Neural Network (CNN) from Scratch,* Data&Stuff, September 5, 2020. https://chrischow.github.io/dataandstuff/2020-09-05-deep-learning-for-aircraft-recognition/
18. Christopher Miller, Mark Draper, Jurriaan van Diggelen, Marlijn Heijnen, Robert J. Shively, Frank Flemisch, Marcel Baltzer, Rogier Woltjer, Mike Boardman, Kate Devitt, Marie-Pierre Pacaux-Lemoine, and Emma Parry, *Meaningful Human Control of AI-based Systems: Workshop Technical Evaluation Report, Thematic Perspectives and Associated Scenarios,*

NATO Science and Technological Organization, June 2023. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-322/$MP-HFM-322-ES.pdf

19. Clara Maathuis and Kasper Cools, *Risk and Control Measures for Building Trustworthy Autonomous Weapon Systems*, International Conference on Cyber Warfare and Security, March 2025. https://www.researchgate.net/publication/390187327_Risks_and_Control_Measures_for_Building_Trustworthy_Autonomous_Weapon_Systems
20. CS Consulting, *Mirco Drones Killer Arms Robots- Autonomous Artificial Intelligence – Warning*, YouTube, November 17, 2017. https://www.youtube.com/watch?v=TlO2gcs1YvM&t=15s
21. Damian Copeland, Rain Liivoja, and Lauren Sanders, *The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems*, Journal of Conflict and Security Law, November 18, 2022. https://doi.org/10.1093/jcsl/krac035
22. Daniele Amoroso and Guglielmo Tamburrini, *Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues*, Current Robotics Reports, August 24, 2020. https://doi.org/10.1007/s43154-020-00024-3
23. Daniele Amoroso and Guglielmo Tamburrini, *Toward a Normative Model of Meaningful Human Control Over Weapons Systems*, Ethics & International Affairs, January 1, 2021. https://doi.org/10.1017/s0892679421000241
24. David Hambling, *The 'Magic Bullet' Drones Behind Azerbaijan's Victory Over Armenia*, Forbes, November 11, 2020. https://www.forbes.com/sites/davidhambling/2020/11/10/the-magic-bullet-drones-behind--azerbaijans-victory-over-armenia/
25. David Hambling, *Ukraine's AI Drones Seek and Attack Russian Forces Without Human Oversight*, Forbes, October 17, 2023. https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/
26. DevX Editorial Staff, *Local Interpretable Modal-Agnostic Explanations*, DevX, January 16, 2024. https://www.devx.com/terms/local-interpretable-model-agnostic-explanations/
27. Emanuela-Chiara Gillard, *Some Reflections on the 'Incidental Harm' Side of Proportionality Assessment*s, Vanderbilt Journal of Transnational Law, May 2018. https://core.ac.uk/download/225543827.pdf
28. Eva von Mühlenen, Zina Chatzidimitriadou, and Andreas Balsiger, *Regulating the Future: Navigating Ethical and Legal Pathways in Brain-Computer Interface Technology,* Sidley

Austin LLP, April 4, 2024. https://www.lexology.com/library/detail.aspx?g=dddd06ab-992a-4634-957d-a5d680797cd9

29. Federal Ministry for Economic Affairs and Climate Action, *Regulatory Sandboxes – Testing Environments for Innovation and Regulation*, BMWK, September 2022. https://www.bmwk.de/Redaktion/EN/Dossier/regulatory-sandboxes.html
30. Frank Sauer, *Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible,* ICRC, March 2021. https://international-review.icrc.org/articles/stepping-back-from-brink-regulation-of-autonomous-weapons-systems-913
31. Grace Sheehan, *Cheap Drones, Expensive Lessons: Ethics, Innovation, and Regulation of Autonomous Weapons Systems,* The Henry M. Jackson of International Studies, University of Washington, July 9, 2025. https://jsis.washington.edu/news/cheap-drones-expensive-lessons-ethics-innovation-and-regulation-of-autonomous-weapon-systems/
32. Grief, Nick, Illingworth, Shona, Hoskins, Andrew and Conway, and Martin A., *The Airspace Tribunal: Towards a New Human Right to Protect the Freedom to Exist Without Physical or Psychological Threat From Above,* Kent Academic Repository, February 16, 2021. https://kar.kent.ac.uk/68733/
33. Heather M. Roff, Magnifying *Human Confusion: Meaningful Human Control and the Ongoing Debate on Autonomous Weapons*, Center for Ethics and The Rule of Law - University of Pennsylvania, May 9, 2024. https://www.penncerl.org/the-rule-of-law-post/magnifying-human-confusion-meaningful-human-control-and-the-ongoing-debate-on-autonomous-weapons/
34. Heather M. Roff, and Richard Moyes, *Meaningful Human Control, Artificial Intelligence and Autonomous Weapons,* Briefing paper prepared for the Informal Meeting of Experts on LAWS, UN Convention on CCW, April 2016. https://article36.org/wp-content/uploads/2016/04/MHC-AI-and-AWS-FINAL.pdf
35. Henrik Syse, *Meaningful Human Control*, Journal of Military Ethics, January 2, 2023. https://doi.org/10.1080/15027570.2023.2235123
36. Human Rights Watch, *Azerbaijan: Attack on Church Possible War Crime,* December 16, 2020. https://www.hrw.org/news/2020/12/16/azerbaijan-attack-church-possible-war-crime
37. Human Rights Watch, *'Killer Robots' Threaten Human Rights During War, Peace*, April 28, 2025. https://www.hrw.org/news/2025/04/28/killer-robots-threaten-human-rights-during-war-peace

38. Human Rights Watch, *Killer Robots and the Concept of Meaningful Human Control*, April 11, 2016. https://www.hrw.org/news/2016/04/11/killer-robots-and-concept-meaningful-human-control
39. Human Rights Watch, *New Weapons, Proven Precedent, Elements of and Models for a Treaty on Killer Robots*, Octobre 20, 2020. https://www.hrw.org/report/2020/10/20/new-weapons-proven-precedent/elements-and-models-treaty-killer-robots
40. IBM, *What is a decision tree*, https://www.ibm.com/think/topics/decision-trees
41. IBM, *What is a neural network, https://www.ibm.com/think/topics/neural-networks*
42. ICRC, *Article 48 – Basic rule,* IHL DATABASES, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-48
43. ICRC, *Article 51- Protection of the civilian population,* IHL DATABASES, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-5
44. ICRC, *ICRC Position on Autonomous Weapon Systems*, International Committee of the Red Cross, January 21, 2022. https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems
45. ICRC, *Legal Review of New Weapons,* April 2021, https://www.icrc.org/sites/default/files/document/file_list/dp_consult_12_legal_review_of_new_weapons.pdf
46. ICRC, *Martens Clause "How Does Law Protect in War?,* Online Casebook, https://casebook.icrc.org/a_to_z/glossary/martens-clause
47. ICRC, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.,* IHL DATABASES, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36/commentary/1987
48. ICRC, *Rules,* IHL DATABASES, https://ihl-databases.icrc.org/en/customary-ihl/v1
49. ICRC, *The Geneva Conventions and Their Commentaries*, ICRC, June 28, 2024. https://www.icrc.org/en/law-and-policy/geneva-conventions-and-their-commentaries
50. ICRC, *United Kingdom, Unlawful Killings In Afghanistan,* How Does Law Protect In War?, Online Casebook, 2022. https://casebook.icrc.org/case-study/united-kingdom-unlawful-killings-afghanistan
51. Ingvild Bode and Tom F.A. Watts, *Loitering Munitions and Unpredictability: Autonomy in Weapon Systems and Challenges to Human Control,* Center for War Studies, May 2023.

https://www.researchgate.net/publication/371351342_Loitering_Munitions_and_Unpredictability_Autonomy_in_Weapon_Systems_and_Challenges_to_Human_Control

52. Ingvild Bode and Tom F.A. Watts, *Loitering Munitions: Flagging an Urgent need for Legally Binding Rules for Autonomy in Weapon Systems,* ICRC, June 29, 2023. https://blogs.icrc.org/law-and-policy/2023/06/29/loitering-munitions-legally-binding-rules-autonomy-weapon-systems/
53. James Dawes, *UN Fails to Agree on 'Killer Robot' Ban as Nations Pour Billions Into Autonomous Weapons Research,* The Conversation, December 20, 2021. https://theconversation.com/un-fails-to-agree-on-killer-robot-ban-as-nations-pour-billions-into-autonomous-weapons-research-173616
54. James Farrant and Christopher Ford, *Autonomous Weapons and Weapon Reviews: The UK Second International Weapon Review Forum*, International Law Studies, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4735498
55. Jennifer Dickey, *Navigating the legal and ethical landscape of brain-computer interfaces: Insights from Colorado and Minnesota,* IAPP, June 11, 2024. https://iapp.org/news/a/navigating-the-legal-and-ethical-landscape-of-brain-computer-interfaces-insights-from-colorado-and-minnesota
56. Jennifer Menninger, *GGE Diskutiert Autonome Waffensysteme in Genf*, IFFF, April 1, 2025. https://www.wilpf.de/2025/04/01/gge-diskutiert-autonome-waffensysteme-in-genf/
57. Jeroen Van Den Boogaard, *Proportionality and Autonomous Weapons Systems*, University of Amsterdam Law School, March 17, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2748997
58. Jonathan Kwik and Tom Van Engers, *Algorithmic fog of war: When lack of transparency violates the law of armed conflict,* Faculty of Law, University of Amsterdam, March 2021. https://www.researchgate.net/publication/350025977_Algorithmic_fog_of_war_When_lack_of_transparency_violates_the_law_of_armed_conflict
59. Jonathan Kwik, *A Practicable Operationalization of Meaningful Human Control*, Faculty of Law, University of Amsterdam, April 28, 2022. https://www.mdpi.com/2075-471X/11/3/43
60. Joseph Clark, *Hicks to See Joint, Combined Command and Control Capabilities in Action During Project Convergence Experiment*, U.S. Department of Defense, February 29, 2024. https://www.defense.gov/News/News-Stories/Article/Article/3691665/hicks-to-see-joint-combined-command-and-control-capabilities-in-action-during-p/

61. Jutta Weber, *Autonomous Drone Swarms and the Contested Imaginaries of Artificial Intelligence*, Digital War 5, January 1, 2024. https://doi.org/10.1057/s42984-023-00076-7
62. Kamala Harris, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, United States Department of State, November 1, 2023. https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy
63. Kenneth Anderson, Daniel Reiner, and Matthew Waxman, *Adapting the Law of Armed Conflict to Autonomous Weapon Systems*, International Law Studies U.S. Naval War College, 2014. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1015&context=ils
64. Lena Trabucco, *What Is Meaningful Human Control, Anyway? Cracking the Code on Autonomous Weapons and Human Judgment*, Modern War Institute, September 21, 2023. https://mwi.westpoint.edu/what-is-meaningful-human-control-anyway-cracking-the-code-on-autonomous-weapons-and-human-judgment/
65. Maciek Zajac, *AWS Compliance with the Ethical Principle of Proportionality: Three Possible Solutions*, Ethics and Information Technology 25, February 13, 2023. https://doi.org/10.1007/s10676-023-09689-8
66. Mariarosaria Taddeo and Alexander Blanchard, *A Comparative Analysis of the Definitions of Autonomous Weapons Systems*, Science and Engineering Ethics, August 23, 2022. https://doi.org/10.1007/s11948-022-00392-3
67. Michael C. Horowitz, *The Ethics & Morality of Robotic Warfare: Assessing the Debate over Autonomous Weapons*, Daedalus, Fall 2016. https://www.amacad.org/sites/default/files/publication/downloads/004_DAED_a_00409-pp025-036.pdf
68. Michael N. Schmitt and Sean Watts, *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*, Texas International Law Journal, 2015. https://core.ac.uk/download/pdf/151188666.pdf
69. Milena Sterio, *Autonomous Weapons Systems and the Need to Update International Humanitarian Law*, Case Western Reserve Journal of International Law, May 06, 2025. https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2702&context=jil
70. Molly Liebergall, *New Investigations Detail Concerns Over Israel's Use of AI in Choosing Targets,* Morning Brew, December 19, 2023. https://www.morningbrew.com/daily/stories/2023/12/20/new-investigations-israel-ai-targets

71. Neil Davidson, *A Legal Perspective: Autonomous Weapon Systems under International Humanitarian Law,* UNODA Occasional Papers, January 2018. https://www.icrc.org/sites/default/files/document/file_list/autonomous_weapon_systems_under_international_humanitarian_law.pdf
72. Nils Melzer, *International Humanitarian Law – A Comprehensive Introduction,* ICRC, February 2017. https://www.jep.gov.co/sala-de-Prensa/Documents/4231_002-IHL_WEB_13.pdf
73. Omar Yousef Shehabi and Asaf Lubin, *Israel – Hamas 2024 Symposium – Algorithms of War: Military AI and the War in Gaza*, Articles of War, January 24, 2024. https://lieber.westpoint.edu/algorithms-war-military-ai-war-gaza/
74. Paul Scharre, *Autonoums Weapons and Stability*, King's College London, April 1, 2020, https://kclpure.kcl.ac.uk/ws/portalfiles/portal/129451536/2020_Scharre_Paul_1575997_ethesis.pdf
75. Paul Scharre, *Autonomous Weapons and Operational Risk.* Center for a New American Security, February 2016. https://www.stopkillerrobots.org/wp-content/uploads/2021/09/CNAS_Autonomous-weapons-operational-risk.pdf
76. Paul Scharre, *Army of None: Autonomous Weapons and the Future of War,* W.W. Norton & Company, 2018. https://wwnorton.com/books/Army-of-None/
77. Peter Asaro, *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-making*, ICRC No.886, June 1, 2012. https://international-review.icrc.org/articles/banning-autonomous-weapon-systems-human-rights-automation-and-dehumanization-lethal
78. Richard Moyes, *Key Elements of Meaningful Human Control*, Article 36 Background Paper for the CCW on LAWS, April 11-15, 2016. https://www.article36.org/wp-content/uploads/2016/04/MHC-2016-FINAL.pdf
79. Shaan Shaikh and Wes Rumbaugh, *The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense,* CSIS, December 8, 2020. https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense
80. SIPRI, *Related publications: Autonomy in weapon systems,* https://www.sipri.org/research/armament-and-disarmament/emerging-military-and-security-technologies/autonomy-weapon-systems/recent-pubs
81. Stop Killer Robots, *2021 Campaign to Stop Killer Robots,* https://www.stopkillerrobots.org

82. Susanne Beck, *Humanity in War? The Importance of Meaningful Human Control for the Regulation of Autonomous Weapons Systems*, Ethics and Armed Forces, January 2024, https://www.ethikundmilitaer.de/en/magazine-datenbank/detail/01-2024/article/humanity-in-war-the-importance-of-meaningful-human-control-for-the-regulation-of-autonomous-weapons-systems
83. Tarisa Kramadibrata Yasin, *Effective human control over lethal autonomous weapons systems and compliance with international humanitarian law*, Bond University, February 2023. https://core.ac.uk/download/589234091.pdf
84. The Center of Ethical Education in the Armed Forces, *Humanity in War? The Importance of Meaningful Human Control for the Regulation of Autonomous Weapons Systems,* Ethics and Armed Forces, January 2024. https://www.ethikundmilitaer.de/en/2024/1-ai-and-autonomy-in-weapons-war-and-conflict-out-of-control/humanity-in-war-the-importance-of-meaningful-human-control-for-the-regulation-of-autonomous-weapons-systems
85. Thompson Chengeta, *Is the Convention on conventional Weapons the appropriate framework to produce a new law on autonomous weapons systems?,* Pretoria University Law Press, March 2023. https://www.pulp.up.ac.za/images/edocman/edited-collections/a_life_interrupted/Chengeta.pdf
86. Ousman Noor, *States make progress on policy at UN discussions, as momentum builds towards Treaty on AWS,* Stop Killer Robots, March 14, 2023. https://www.stopkillerrobots.org/news/states-make-progress-on-policy-at-un-discussions-as-momentum-builds-towards-treaty-on-aws/
87. UK Stop Killer Robots, *UK Must Lead, Not Lag, on Regulating Autonomous Weapons*, July 22, 2025. https://ukstopkillerrobots.org.uk/news/
88. United Nations, *Meetings of the Group of Governmental Experts,* UNODA DATABASES, https://disarmament.unoda.org/meetings-of-the-group-of-governmental-experts/
89. U.S. Department of Defense. *DoD Directive 3000.09 – Autonomy in Weapon Systems,* January 25, 2023. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf
90. Vincent Boulanin, *Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems,* SIPRI No.2015/1, November 2015. https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1501.pdf
91. Vincent Boulanin, Netta Goussac, and Laura Bruun, *Autonomous Weapon Systems and International Humanitarian Law: Identifying Limits and the Required Type and Degree of Human–Machine Interaction*, SIPRI, June

2021. https://www.sipri.org/publications/2021/policy-reports/autonomous-weapon-systems-and-international-humanitarian-law-identifying-limits-and-required-type

92. Vincent Boulanin, Moa Peldán Carlsson, Nette Goussac, and Neil Davison, *Autonomy in Weapon Identifying Practical Human Control,* SIPRI, June 2020. https://www.sipri.org/publications/2020/policy-reports/limits-autonomy-weapon-systems-identifying-practical-elements-human-control
93. Vincent Boulanin, and Maaike Verbruggen, *Mapping the Development of Autonomy in Weapon Systems,* SIPRI, November 2017. https://www.sipri.org/publications/2017/policy-reports/mapping-development-autonomy-weapon-systems
94. Vincent Boulanin, Kolja Brockmann and Luke Richards, *Responsible Artificial Intelligence Research and Innovation for International Peace and Security,* SIPRI, November 2020. https://www.sipri.org/publications/2020/policy-reports/responsible-artificial-intelligence-research-and-innovation-international-peace-and-security
95. Yuval Abraham, *A Mass Assassination Factory': Inside Israel's Calculated Bombing of Gaza*, +972 Magazine, April 25, 2024. https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/
96. Yuval Shany, *Red Herring, Meaningful Human Control and the Autonomous Weapons Systems Debate*, Ethics in AI, March 18, 2024. https://www.oxford-aiethics.ox.ac.uk/blog/red-herring-meaningful-human-control-and-autonomous-weapons-systems-debate