

INTERNATIONAL LAW AT THE TECHNOLOGICAL FRONTIER

Edited by Gökhan **Güneysu,** Sezercan **Bektaş** & Merve **Erdem Burger**

SAKARYA UNIVERSITY
PRESS

International Law at the Technological Frontier

Edited by

Gökhan Güneysu
Sezercan Bektaş
Merve Erdem Burger

SAKARYA UNIVERSITY

PRESS

EDITORS

Gökhan Güneysu
Department of International Law
Faculty of Law
Anadolu University, Eskisehir, Türkiye
gguneysu@anadolu.edu.tr
0000-0002-1754-953X

Sezercan Bektaş
Department of International Law
Faculty of Law
Sakarya University, Sakarya, Türkiye
sezercanbektas@sakarya.edu.tr
0000-0001-7395-5375

Merve Erdem Burger
Independent Space Law and Policy Consultant
Co-Founder, Swiss Space Law Forum
Switzerland and Türkiye
merverdemburger@gmail.com
0000-0001-6085-5308

AUTHORS

Adem Özer
0000-0002-6443-1032

Annie Kazarján
0009-0009-6025-9376

Aurora Giannone
0009-0005-3186-4754

Balázs Bartóki-Gönczy
0000-0002-2147-901X

Görkem Kayacık
0000-0001-7530-2722

İbrahim Demir
0009-0009-6573-7250

Merve Erdem Burger
0000-0001-6085-5308

Merve Küçük
0000-0003-2894-6087

Nebile Pelin Mantı
0000-0001-7124-7850

Neslihan Özkerim Güner
0000-0001-8130-9461

Sezercan Bektaş
0000-0001-7395-5375

Şenel Sarsıkoğlu
0000-0002-2204-8422

International Law at the Technological Frontier

Editors

Gökhan Güneysu, Sezercan Bektaş & Merve Erdem Burger

Keywords

1. Law and Technology, **2.** Emerging Technologies,
3. Autonomous Systems, **4.** Global Commons

Sustainable Development Goals



E- ISBN: 978-605-2238-93-6
DOI: 10.59537/saupress.2608
Sakarya University Publication No: 262
Published Online in November 2026
1st Edition, November 2026
Publishing Director: *Mahmut Akyiğit*
Layout Design: *Mustafa Kemal Köse, Hüseyin Avni Yazıcı*
Language Editing: *Ayşegül Yolcu, Funda Çankaya, and Muhammet Şibli Adalı*

Sakarya University Press

Address
Sakarya University, Scientific Publications Office, B2 Block, 54050 Serdivan, Sakarya/Türkiye
https://sauyayinlari.sakarya.edu.tr

This work is published under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0). The book may be copied, adapted, distributed, and reused for non-commercial purposes, provided that appropriate attribution is given.

The complete manuscript of this book has undergone peer review to ensure high academic standards. For further information, please refer to the publisher's Reviewer Guide.

Competing Interests: The authors have no competing interests to declare.

Disclaimer: The views and interpretations expressed in this publication are solely those of the author(s) and do not necessarily reflect the official positions of the publisher or any affiliated institutions. The publisher assumes no responsibility for these views and interpretations.

The content of this publication has not been approved by the United Nations and does not necessarily reflect the views of the United Nations, its officials, or its Member States.

The cover image was generated using ChatGPT by OpenAI.

CONTENTS

FOREWORD ..... **vii**

INTRODUCTION **1**

Chapter 1
Legal Governance of Sustainability in the Earth's Orbits.....11
Merve Erdem Burger, Balázs Bartóki-Gönczy, Annie Kazarján

Chapter 2
Space for Sustainability: From Orbital Pollution to Climate Solutions Through Technology and International Law.....40
Aurora Giannone

Chapter 3
Autonomous Ships, the Development of MASS Code and its Legal Implications.....66
Neslihan Özkerim Güner

Chapter 4
Expressive Opinio Juris: The Evidentiary Role of Social Media in the Formation of Customary International Law.....86
Merve Küçük

Chapter 5
Transformation of the Battlefield: A Review of AI-Enabled Cyber Attacks Under International Humanitarian Law.....103
Nebile Pelin Mantı, Adem Özer

Chapter 6
Fiber-Optic Tethered Unmanned Aerial Vehicles in the Context of Environmental Protection During International Armed Conflict.....170
Görkem Kayacık

Chapter 7
An Assessment of Violations of International Humanitarian Law Arising from the Use of Unmanned Combat Aerial Vehicles.....189
İbrahim Demir

Chapter 8
Autonomous Weapons and Individual Criminal Liability in International Criminal Law.....205
Şenel Sarsıkoğlu

Chapter 9
Conclusion and Future Outlook.....232
Sezercan Bektaş

EDITORS AND AUTHORS..... 245

INDEX..... 252

CHAPTER 8

Autonomous Weapons and Individual Criminal Liability in International Criminal Law

Şenel Sarsıkoğlu[1]

The increasing use of autonomous weapon systems (AWS), including lethal autonomous weapons (LAWS) and artificial intelligence-based unmanned aerial vehicles (AI-based drones), raises new legal issues regarding the regime of responsibility under international criminal law (ICL). The fact that these systems can carry out target selection and intervention without human involvement creates uncertainties regarding how criminal liability should be assigned for acts that violate international humanitarian law and human rights law.

The study analyzes the main challenges regarding the establishment of individual criminal liability in instances where autonomous weapon systems are involved in war crimes or crimes against humanity. It assesses the roles and potential responsibilities of programmers, manufacturers, military leaders, and government officials under the Rome Statute within the framework of criminal law. The fact that current regulations do not provide sufficient clarity concerning the material and mental elements of the crime, coupled with the lack of mechanisms to assign liability, creates a substantial gap that complicates identification of responsible parties in cases where AWS result in unlawful harm.

The study also highlights normative deficiencies arising from the utilization of AWS concerning control, accountability, predictability, and mental considerations. Therefore, it implies that reduced human control over AWS may complicate the attribution of culpability to particular individuals. Based on the current legal stance, a framework is proposed for assessing individual criminal liability in AWS incidents. It also addresses the ethical and political issues of entrusting machines with decisions about life and death, and highlights the urgent necessity for new regulations, particularly at the level of international treaties. Thus, by pinpointing legal gaps, the interplay between emerging technologies and ICL is being redefined, establishing a conceptual foundation for future regulatory frameworks.

1 Kastamonu University, Faculty of Economics and Administrative Sciences, Department of International Relations, Division of Public International Law, Kastamonu, Türkiye, senels@kastamonu.edu.tr

Cite as: Sarsıkoğlu, Ş. (2026). Autonomous weapons and individual criminal liability in international criminal law. In G. Güneysu, S. Bektaş, & M. Erdem Burger (Eds.), *International law at the technological frontier* (pp. 205–231). Sakarya University Press. https://doi.org/10.59537/saupress.2617

Introduction: Next-Generation Warfare Technologies Pushing the Boundaries of the Legal Framework

The rise of autonomous weapon systems on modern battlefields signifies not merely the introduction of a novel weapon type but also a fundamental shift that influences both the conduct of hostilities and the framework of legal liability (Campani Farias, 2025, p. 2; Güneysu, 2024b, p. 395; Shulzhenko & Romashkin, 2021, p. 72). The rapid pace of development and potential consequences of these technologies are often characterized in the literature using the "Oppenheimer moment" analogy, which, akin to the development of the atomic bomb, combines the promise of strategic superiority with a cautionary note regarding existential threats to humanity (Frunzeti et al., 2025, p. 4; Westhues, 2025, p. 130). AWS, capable of selecting targets and engaging without human intervention, challenges the applicability of traditional mechanisms used to determine individual criminal responsibility for war crimes and crimes against humanity (Güneysu, 2024b, p. 397; Shulzhenko & Romashkin, 2021, p. 72). In this context, the decision-making hierarchy involving humans and machines is being reshaped, resulting in ambiguous lines of accountability among commanders, operators, programmers, manufacturers, and policymakers (Petersen, 2024, p. 286; Rotsch, 2009, p. 549). This increases the risk of attributing an unlawful act to a machine behavior rather than to a human, thereby raising the possibility of a liability gap and impunity (Campani Farias, 2025, p. 2; Güneysu, 2024b, p. 400). It also entails the risk of eroding the deterrent capacity and normative authority of international humanitarian law (Aksenova, 2014, p. 2; Güneysu, 2025, p. 7). However, the notion of a culpability gap should not automatically lead us to the inevitable conclusion of impunity (Kwik, 2023, p. 2). This study contends that the responsibility gap associated with AWS does not necessarily require the establishment of a new legal regime; instead, it can be substantially reduced through a systematic and purposive interpretation of existing doctrines (Aksenova, 2014, p. 1; Renzikowski, 2021, p. 92; Rotsch, 2009, p. 549).

In this respect, two main issues emerge. The first issue is how to apply the Rome Statute's framework of individual responsibility in light of the technological features of AWS (Shulzhenko & Romashkin, 2021, p. 72). This line covers discussions regarding the mental element of a crime and the forms of participation (Aksenova, 2014, p. 1). The second issue is identifying the limits within which control-based approaches can be applied in the context of AWS for establishing the accountability of senior decision-makers. At this point, the organizational dominance theory (Organisationsherrschaftslehre) developed in German criminal law serves as an important reference point (Rotsch, 2009, p.

549). In addition, an expanded interpretation of commander responsibility, tailored to the development, procurement, deployment, and operational phases of AWS, is among the instruments that can narrow the responsibility gap (Aksenova, 2014, p. 1). At this point, there is a need for technical and organizational standards to be implemented by governments. Record-keeping, auditing, accountability, and limiting the context of use are prime examples of these standards (Campani Farias, 2025, p. 2). Such standards strengthen the evidential basis of liability evaluation by increasing the predictability and transparency. In the study, AWS are defined as weapon systems that, once triggered, can autonomously identify, select, and engage targets without human involvement (Güneysu, 2024b, p. 398). The definition focuses on the function of the system rather than its design and encompasses systems that can result in both lethal and non-lethal outcomes.

8.1. Autonomous Weapon Systems (AWS) and Basic Principles of International Law

To comprehend the legal issues posed by the technological revolution, the core characteristics of autonomous systems and their impact on traditional legal structures must be identified. The existing international legal system has been designed with human decision-making processes in consideration (Petrović et al., 2024, p. 31). The distinctive technological features of AWS make them not only more advanced than conventional weapon systems but also instruments that structurally challenge legal assessments (Westhues, 2025, p. 112). The conduct of target selection and use-of-force decisions without meaningful human control, or within a framework in which the human role is significantly diminished, directly affects the implementation of the principles of distinction, proportionality, and precaution, as well as the establishment of individual criminal responsibility (Kersten, 2025; Kwik, 2023, p. 2). That is why the focus of the AWS debate is not limited to an artificial intelligence (AI) issue. The determining factors are the stage at which the human is involved in the decision-making chain, as well as the extent and supervisory capacity of that engagement (Campani Farias, 2025, p. 2; Moyes, 2016, p. 239).

8.1.1. Definition and Classification of Autonomy

Autonomous systems are distinguished from automatic systems by their ability to operate beyond predetermined rules. These systems can assess fluctuating environmental conditions, select among alternatives, and continue task execution without human intervention (Suchman, 2016, p. 273). Accordingly, autonomy cannot be regarded as a binary category. It is a spectrum that varies according to the degree of human control (Boulanin, 2016, p. 26).

What distinguishes autonomous systems from automatic systems is not merely that they operate based on predefined rules. For this reason, autonomy is not a binary category. It is a spectrum that fluctuates according to the extent of human control. At one extreme are systems that are either controlled or approved by humans. At the opposite end are systems that execute the full task cycle autonomously, without human interaction (Petrović et al., 2024, p. 10; Westhues, 2025, p. 117). From an IHL perspective, what is decisive is not whether the system is considered autonomous, but to what extent the human role is bypassed in critical functions such as target selection and the application of force (Westhues, 2025, p. 127). This approach allows the discussion to be framed in a normatively accurate way (Moyes, 2016, p. 240). This is due to the fact that as human involvement in crucial operations diminishes, evaluating legality and attributing criminal liability become progressively challenging. State practices and policy documents indicate that there is no singular, universally accepted definition of AWS (Boulanin, 2016, p. 26; Westhues, 2025, p. 111). Some approaches define autonomy broadly and encompass human-supervised and semi-autonomous systems within the scope of the definition. Others, however, require higher thresholds, introducing criteria such as a capacity for higher-level goal comprehension and thereby removing many systems from the definition (Dahlmann, 2016, p. 36). Certain actors, such as China, adopt an even narrower perspective, placing emphasis on elements such as irreversibility of the system once initiated and the existence of autonomous learning capabilities (Campani Farias, 2025, p. 2; Jenks, 2016, p. 177). These differences are not merely terminological; rather, they reflect strategic choices that expand or restrict the scope of regulation. The ambiguity in the definition is also evident in discussions surrounding meaningful human control, a concept that in some debates is deliberately left vague.

AWS are weapon systems capable of selecting targets and applying force to them without meaningful human control (Mann, 2019; Westhues, 2025, p. 112). These systems perceive their environment, adapt to changing conditions, and can make decisions within predetermined constraints. Lethal autonomous weapons (LAWs) refer to a form of these capabilities designed for the purpose of using lethal force. There are three models based on the degree of human intervention (Güneysu, 2024b, p. 407; Kersten, 2025; Westhues, 2025, p. 117).

In human-controlled systems, the system determines the target, but the decision to use force rests with the human (Coco, 2023, p. 1079). Semi-autonomous systems, on the other hand, can determine the target themselves and use force, but the operator monitors the process, vetoes the decision if necessary, or intervenes (Coco, 2023, p. 1079; Westhues, 2025, p. 117). In fully autonomous systems, the targeting and force application cycle is completed

without human intervention after activation (Petrović et al., 2024, p. 10). In recent years, the emphasis on meaningful human control has become more prominent in the United Nations (UN) system and on international platforms, and this emphasis is addressed alongside discussions on risk management and accountability. From a criminal law standpoint, this variability indicates that the same technology may be employed in scenarios involving varying human roles. Consequently, criminal culpability must be assessed based on the context of use and the existing control mechanisms.

8.1.2. The Black Box Issue: Opacity and Unpredictability

In AWS based on machine learning and neural networks, decision-making processes often exhibit an opaque character (Greipl, 2023, p. 1101; Güneysu, 2025, p. 2; Kersten, 2025; Kwik, 2023, p. 1). In some instances, the reasons why a system produces a particular output in response to a given input are not fully explainable even to its developers (Greipl, 2023, p. 1102; Kersten, 2025). The issue here is not the predictable operation of a rule-based mechanism. Decisions are formulated based on context-sensitive and complex patterns extracted from training data. This opacity increases the risk of behavioral unpredictability, particularly under unusual environmental conditions or in scenarios that do not align with the training data. Instances of how classification errors in civilian technologies can lead to fatal consequences illustrate the necessity of a more rigorous assessment of this risk in the military domain (Geiß, 2016, p. 109; Kwik, 2023, p. 9). This situation directly affects two fundamental components of international criminal law. The first concerns the issue of how the element of knowledge and the threshold of predictability are to be established with respect to the mental element. The second pertains to the question of to which individual the unlawful act constituting a crime can be attributed, and through which role and level of control such attribution can be determined (Güneysu, 2025, p. 2; Kwik, 2023, p. 1; Mann, 2019).

The issue regarding the culpability regime under the Rome Statute is clear. When the decision-maker's actions are carried out through a system that is opaque and not fully predictable, it is controversial by which criteria it should be determined to what extent the decision-maker foresaw, or could objectively be expected to have foreseen, a concrete violation of IHL (Guo, 2025, p. 31). This is not merely a theoretical debate about mental principles, but it is also a matter of evidence and proof (Guo, 2025, p. 31). As opacity increases, the attribution of liability shifts from the instant of the decision to the foundational preferences of the system. Within this framework, the selection, delimitation, and testing of the system as well as the specification of task parameters, the management of updates, and the design of intervention capabilities become key

factors (Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems [GGE], 2022). This technological reality underpins the basis for the de lege lata analysis and de lege ferenda recommendations to be presented in the subsequent sections.

8.1.3. AWS in Light of the Fundamental Principles of International Humanitarian Law

For individual criminal liability to be considered, there must first be a violation under IHL (Ohlin, 2013, p. 82). Therefore, the extent to which AWS usage complies with the principles of distinction, proportionality, and precautions forms the basis for liability assessment (Australia et al., 2021; Güneysu, 2024a, p. 141). Indeed, the applicability of these principles constitutes the primary benchmark for determining whether an AWS can be legitimately constructed and utilized in specific cases. The principle of distinction requires a constant differentiation between civilians and combatants, as well as between civilian objects and military targets (Güneysu, 2024a, p. 144; Ohlin, 2013, p. 85). AWS's ability to fulfill this obligation faces significant challenges due to the dynamic nature of the battlefield and the limitations of sensors and algorithms (Guo, 2025, p. 30). Particularly in urban conflicts, the ability to distinguish algorithmically, in real time and with accuracy, between a civilian directly participating in the conflict and a civilian who happens to be in the area is questionable with current technology. Likewise, it is difficult to reliably distinguish between a soldier who has surrendered and an active combatant based on sensor data (Monnett, 2024, p. 4). The system's resilience against deception and masking techniques, as well as its capacity to prevent mistargeting, further increases the risk of violating the principle of distinction. Whether a weapons system is considered inherently unlawful (per se unlawful) does not depend solely on its technical characteristics, as the intended context of use is also a determining factor (Güneysu, 2024a, p. 138). The same technology can result in different risk profiles depending on the context. The principle of proportionality prohibits attacks that cause excessive civilian casualties and damage relative to the expected concrete and direct military advantage (Guo, 2025, p. 31; Ohlin, 2013, p. 82). This is not merely a quantitative calculation as it requires qualitative and context-sensitive judgment (Guo, 2025, p. 29). This is because the assessment of the balance between military advantage and incidental civilian harm involves moral, strategic, and legal judgments that cannot be reduced to measurable metrics. Assessing how the military advantage anticipated from a target should be balanced against potential civilian harm that may occur in nearby schools, markets, or residential areas, and at what point such harm would be deemed excessive, constitutes a form of human judgment that surpasses the

limits of contemporary artificial intelligence capabilities (Guo, 2025, p. 32). For this reason, the principle of proportionality represents one of the most challenging thresholds from an AWS perspective.

The precautionary principle mandates that all feasible measures be taken to protect civilians and civilian objects during the planning and execution of an attack. This includes verifying the military status of the target, selecting weapons and methods that cause the least harm to civilians, and canceling or postponing an attack if it is deemed disproportionate (Lee, 2025). With regard to AWS, the discussion of precautions arises in two dimensions (Kakko, 2022, p. 13). First, especially in machine-learning–based black-box systems, the inability to explain the decision-making logic leads to insufficient predictability in the system's behaviour. This, in turn, complicates the commander's ability to assess the consequences and to effectively implement precautionary measures (Kakko, 2022, p. 12). The second relates to the expansion of the temporal scope of the precautionary obligation (Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects [Meeting of the High Contracting Parties], 2019, p. 10). Since the behaviour of the system is predominantly shaped during the stages of design, development, programming, testing, and validation, the obligation to take precautions extends beyond the moment of attack and encompasses all phases preceding deployment (Meeting of the High Contracting Parties, 2019, p. 10). Putting a system with insufficient predictability into operational use is a problematic choice from the perspective of the obligation to take precautions (International Committee of the Red Cross [ICRC], 2021). A common feature of these three principles is that they have contextual and open-to-interpretation structures. This effectively makes the behaviour of AWS more difficult to predict. This unpredictability is directly associated with the determination of the components of a crime, especially the mental component. In these instances, it becomes considerably more challenging to demonstrate that a military commander or programmer planned or was aware of the unlawful effect.

8.2. Individual Criminal Responsibility: The Uncertainty of the Material and Mental Elements

8.2.1. With Respect to Material Elements

If an AWS attack leads to an act that violates IHL, such as civilian death or an attack on a protected object, the first inquiry is to whom that act should be attributed. In criminal law, attribution necessitates the existence of a conduct directed toward the commission of a violation. In crimes involving a specific

result, a causal connection must also be established between the conduct and the resulting harm (Lee, 2025). In the context of AWS, the problem is not merely the weakening of this causal link. The conduct cannot be fixed at a specific point. The components of the act are dispersed across different actors and time frames. The unlawful outcome arises from a disjointed pattern of behavior that cannot be attributed to the actions of a single perpetrator (Bauer, 2016, p. 231). In many cases, the process leading to a violation in AWS does not stem from a single human act. It is shaped by a combination of data selection, model training, testing protocols, software updates, the target pool, engagement authorization, and real-time sensor inputs (van den Bosch & Roelofs, 2025, p. 15-6). In this process, each of the actors—such as the programmer, manufacturer, commander, and operator—makes a contribution that is necessary but not sufficient on its own to produce an unlawful outcome (Lee, 2025; van den Bosch & Roelofs, 2025, p. 15-6). Additionally, AWS's ability to adjust to its environment and, in some cases, to learn can cause it to deviate from the initial human direction. This makes it even more complicated to attribute the outcome to the actions of a particular individual (van den Bosch & Roelofs, 2025, p. 15-6).

This fragmented nature creates two types of structural problems in proving the material element, starting from a break in the chain of responsibility. The contributions to responsibility among the coder, manufacturer, commander, and operator become fragmented (van den Bosch & Roelofs, 2025, p. 15-6). Each person remains in a position where they can claim to have contributed only in technical, logistical, or operational terms. This distance complicates the concentration of the link between the conduct and the result in a particular individual and renders legal attribution open to debate (Bauer, 2016, p. 231). Secondly, a systemic behavior issue arises in addressing the material element. In complex and dynamic combat environments, the predictability of system outputs may decrease (van den Bosch & Roelofs, 2025, p. 15-5). This situation not only undermines the assessment of causality but also complicates the examination of culpability and mental elements, as it is not possible to establish concretely which decision parameter or which contributing factor resulted in the outcome (Kakko, 2022, p. 12). At this point, the decisive issue in attributing the unlawful outcome to a human act is how to apply the substantial contribution criterion, which is prominent in the Rome Statute (Lee, 2025). Assessing whether an individual has made a substantial contribution to the commission of a crime is particularly challenging in the context of AWS, since the relevant decision-making processes are distributed among multiple actors and occur over extended periods of time. The commander's orders and authorization, the programmer's coding and model choices, the manufacturer's design decisions, and the operator's act of activation all relate to the same result (van den Bosch

& Roelofs, 2025, p. 15-6); however, each contributes to that result to a different degree. The weakening or actual disruption of the causal relation makes it more difficult to prove the material element and deepens the debate over the gap in liability (Lee, 2025). In our view, the evaluation of the material element in the context of AWS should not be confined to the identification of a single act. Indeed, the processual fragmentation of conduct, the temporal dispersion of contributions, and the unpredictability of system consequences necessitate a model of attribution that takes these factors into account together.

8.2.2. With Respect to Mental Elements

Pursuant to Article 30 of the Rome Statute, the material elements of a crime must be committed with intent and knowledge in order to establish individual criminal responsibility (Chaitidou, 2016, p. 833). In this regard, it is based on the notion of intending the result or acting with the knowledge that the outcome will occur as a natural consequence of events. However, the jurisprudence of the International Criminal Court (ICC) and the doctrine are not uniform as to whether Article 30 covers dolus eventualis or the acceptance of risk (Bauer, 2016, p. 233). A clear divergence in interpretation has emerged, particularly regarding the decisions of the pre-trial chamber (Chaitidou, 2016, p. 829). This uncertainty makes it even more difficult to establish the mental element in AWS cases. For this reason, in our view, the discussion of the mental element in the context of AWS often gets locked into the dichotomy of "no knowledge, no responsibility". However, the real issue lies at the level of uncertain yet meaningful risk (Kakko, 2022, p. 13). The approach to evaluating the degree of mental element suggests that in most cases, the gap in liability does not reside at the level of intent or inevitability, but rather in a gray realm that does not fit into the traditional categories of knowledge and intent, due to technical opacity and operational uncertainty, despite awareness of a specific risk (Kwik, 2023, p. 1). In this grey realm, two structural characteristics of AWS are decisive, starting with its unpredictability (van den Bosch & Roelofs, 2025, p. 15-5). In machine learning-based systems, as field conditions and real-time inputs change, system outputs may exhibit unpredictable behavior not anticipated during the testing phase (van den Bosch & Roelofs, 2025, p. 15-6). In such cases, it becomes difficult to prove that the commander, developer, or decision-maker in the supply chain knew that a particular unlawful outcome would occur as part of the normal course of events. In addition to unpredictability, AWS's second defining characteristic is diminished cognizability. The "black box" nature of the system makes it difficult for people to understand what data the system relies on and what internal reasoning it uses to make targeting decisions. This, in turn, undermines the ability to concretize the knowledge element (van den Bosch

& Roelofs, 2025, p. 15-6). However, cognitive impacts such as diminished attention and overreliance on the automation system further complicate the establishment of the mental element. For instance, human operators and decision-makers may tend to be overly reliant on the output of autonomous systems, which directly impacts the discourse surrounding the "knowing and willing" issue related to risk perception (Bo et al., 2022, p. 49).

In light of this information, two flawed approaches emerge in practice. The first approach interprets Article 30 broadly and includes the relevant scope based on the criterion that "it should have foreseen all persons involved in the technical process". However, the objectification of intent in this manner gives rise to concerns with regard to the principle of legality and the principle of personal culpability (Bo et al., 2022, p. 49). The second flawed approach interprets Article 30 narrowly, thereby turning technical complexity and unpredictability into a shield of irresponsibility. This approach carries the risk of creating a de facto zone of impunity by deeming the consequences arising, particularly in complex systems, to be beyond the control of the perpetrator (Bo et al., 2022, p. 49). In our point of view, the solution does not lie in broadening the concept of intent. In a concrete case, a methodology based on verifiable criteria is necessary to determine the stage and the relevant actors involved in the concentration of control over the conduct and understanding of the risk. In this regard, the "ordinary course of events" criterion in Article 30 should be applied in AWS cases not as a subjective attempt to read minds, but as a matter of attribution grounded in concrete evidence regarding institutional knowledge, decision-making chains, and authorization processes. Authorization decisions taken despite firearm examination reports, test results, field analyses, update notes, mission parameters, rules of engagement, and risk warnings are the primary data sources that concretize the knowledge element in terms of the mental element. This approach, without automatically excluding the mental element due to technical ambiguity and without excessively broadening it to undermine the principle of culpability, establishes a verifiable basis for assessing the concentration of control and risk awareness, as well as the actors involved, through documentary evidence and institutional decision-making procedures.

8.2.3. With Respect to Different Actors

From the perspective of the Rome Statute, responsibility for violations arising from AWS largely depends on the extent to which the modes of participation (Öztürk, 2023, p. 269; Tezcan et al., 2023, p. 530) set out in Article 25 and the doctrine of command responsibility provided for in Article 28 can be applied in light of technological developments. In the context of AWS, the 'trigger-puller' metaphor becomes inadequate because the conduct is executed through a chain

of sensors, algorithms, and effectors. Nevertheless, the assessment of liability is based not on participation in the physical commission of the act, but on the concept of control over the act and the crime (Öztürk, 2023, p. 267).

From the perspective of Article 25 of the Rome Statute, direct perpetration is theoretically possible; however, what matters is who holds the power. Furthermore, the focus is not solely on a singular moment of activation, but on the components involved in defining the parameters of the task, selecting the context of use, understanding system constraints, maintaining the capacity to intervene, and actually putting these capabilities into practice (Bo et al., 2022, p. 37). The approach to control-over-the-act, which draws on German legal doctrine, holds that a person who does not personally commit the crime may still be considered a perpetrator if they have a determinative effect on whether the crime is committed and how it is committed (Öztürk, 2023, p. 260). This approach appears theoretically relevant in structures involving many participants, such as AWS, because it attributes liability not to the person who pulls the trigger, but to the one who establishes decisive control over the perpetration of the crime. However, when it comes to the practice, two main problems arise. Since the control conducted by technical personnel often remains at a general capacity level, it becomes difficult to link it to a specific operational violation (Bo et al., 2022, p. 38). Furthermore, the disparity between software and algorithm design and the actual outcomes in the field complicates the burden of proof regarding both relation of causality and mental element. Accordingly, the applicability of Article 25 in the context of AWS depends on establishing that the technical contribution goes beyond a merely theoretical possibility and gives rise to a predictable risk in the concrete instance (Shulzhenko & Romashkin, 2021, p. 77).

The other modes of liability under Article 25 must also be assessed separately in the context of AWS (Shulzhenko & Romashkin, 2021, p. 75). Although the commander is aware that the system's discrimination capacity is insufficient, his decision to deploy the AWS in a densely populated civilian area can be considered an act of command or inducement based on the facts (Chaitidou, 2016, p. 833). With regard to providing assistance, the contributions of developers, programmers, and manufacturers should not be limited to purely technical contributions. It is required that the contribution facilitate the commission of the crime knowingly and willingly (Chaitidou, 2016, p. 834). The mental element that the Rome Statute requires in this regard often poses a significant burden of proof due to the dual-use nature of AWS development efforts (Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate

Effects, 2017). The goal of an AWS developer is often not to facilitate a specific war crime, but to build a system that meets the technical specifications (Lee, 2025). Nevertheless, in certain cases, individual responsibility may become concretized. This concretization entails modifying the system to address a specific violation, intentionally concealing known biases or defects, rendering risk warnings ineffective, or designing the system specifically for a case that is clearly unlawful. Moreover, pursuant to Article 25(3)(d), culpability for contribution to a collective crime may also arise. In particular, continuing to use the system despite being aware that it systematically causes civilian harm can ignite this debate (Shulzhenko & Romashkin, 2021, p. 77).

Command responsibility under Article 28 of the Rome Statute is, in the context of AWS, both the most appropriate normative basis for liability and one of the most commonly misinterpreted areas. The traditional approach bases the commander's responsibility on effective control, the crossing of a certain threshold of knowledge, and a violation of the duty to prevent the crime or punish the perpetrators (Lee, 2025). In the context of AWS, the first issue concerns whether the system can be regarded as a subordinate (Lee, 2025). However, the notion of control under Article 28 cannot be confined to hierarchical command authority over personnel alone. In the context of AWS, control is concretized through the deployment of the system and through effective management over targeting parameters, operational restrictions, and intervention mechanisms (Asaro, 2025; Gjorgjinski, 2021). If this interpretation is not embraced, the assessment swings to one of two possible outcomes. Either the commander's liability is entirely excluded on the grounds of technical difficulties, resulting in de facto impunity, or an unlimited expansion emerges that undermines the principle of fault (Schünemann, 2006, p. 304). The principle that commanders must be aware of Article 28 imposes on them the obligation to perform an effective assessment of the system's capabilities, limitations, and operational risks, and to implement the necessary precautions. Nonetheless, the limits of this obligation must be determined by taking into account the degree to which effective control and pertinent knowledge are concentrated, and among which individuals, in the particular instance.

For government officials and high-level decision-makers, the scope of responsibility appears even more complex (Weigend, 2011, p. 98). Directly linking the actions of political leaders who authorize the development, procurement, or use of an AWS to a specific war crime typically gives rise to significant evidentiary challenges regarding causation and the mental element. For this reason, the debate often remains confined to the level of political responsibility (Guo, 2025, p. 28; Kwik, 2023, p. 1). However, if specific conditions are present—such as the existence of authoritative

decision-making about operational usage scenarios, the incorporation of risk knowledge in records and documentation, and the ongoing occurrence of violations—criminal culpability under Article 25 may come into consideration (Weigend, 2011, p. 92).

In addition to the points mentioned above, there is another key structural feature that complicates liability assessment in the context of AWS. Responsibility is shared among many individuals. When combined with the system's opaque decision-making processes, this gives rise to a feedback dynamic that operates at the organizational level (Guo, 2025, p. 29). Unless it can be clearly established which datasets and decision-making principles are used to generate the system output, liability can be shifted to another decision-making chain for each individual (Guo, 2025, p. 31). This situation creates a practical area of resistance in establishing attribution, particularly in proving the knowledge element. Cognitive tendencies, such as automation bias, further exacerbate the situation. These tendencies make it difficult to assess the perception of risk and to demonstrate the extent to which risk information is reflected in decision-making processes (Güneysu, 2024b, p. 410). Consequently, liability models within the framework of AWS cannot be resolved exclusively through doctrinal analysis. The primary concern is to create an evidentiary framework utilizing records and audits to monitor the concentration of control, the generation of risk information, and the basis for authorization decisions.

8.3. As a Possible Solution: The Doctrine of Control Over the Organization

8.3.1. Roxin's Doctrine of Control over the Organization (Organisationsherrschaftslehre)

In cases where traditional forms of criminal responsibility and complicity face difficulties in attribution and proof in the context of AWS, Claus Roxin's theory of indirect perpetration through organizational control becomes particularly significant. This methodology lays the foundation for attributing responsibility to a high-ranking individual—who does not directly execute the act but effectively directs it through a power structure—as an indirect perpetrator (Weigend, 2011, p. 97). From the perspective of Turkish penal law theory, this model also makes it possible for a person who does not directly participate in the commission of the act to be considered a perpetrator based on their control over the course of action and their power to influence the outcome. Roxin's approach offers an explanation that adapts the theory of control of the crime in cases of indirect perpetration to organizational structures (Weigend,

2011, p. 93). Therefore, indirect perpetration is defined by the person behind the individual who carries out the crime, establishing decisive control over the course of the act and its outcome. In doctrine, this form of control is elucidated by the presence of a structured power infrastructure, the interchangeability of direct perpetrators, and the presumption that orders will be carried out with a high degree of certainty (Weigend, 2011, p. 97).

In the context of AWS, the reason why this doctrine is brought into discussion is that, in certain use scenarios, the idea of conceiving the system as an instrument partially aligns with the conceptual logic of the doctrine (Orozco López, 2021, p. 234; Roxin, 2006, p. 296). However, it is inappropriate to consider AWS as an instrument that can be automatically replaced, just like human workers. This is only possible under certain factual and normative conditions (Roxin, 2006, p. 299). The first condition is that control must not be confined to mere ownership of the technology or general command authority. It must be evidenced that control is effectively centralized over deployment parameters and intervention capabilities (Weigend, 2011, p. 109). In other words, control is concretized through deployment and operational parameters (Ayrancı, 2022). The second condition is that it must be asserted that the system's capabilities and limitations are known or made clear in the specific context of use. This issue is crucial both for upholding the principle of culpability and from the perspective of the logic of proof. If access to information regarding technical capabilities and limitations—and how this information is reflected in decision-making processes—cannot be reflected, any claim of control remains suspended on a normative basis (van den Bosch & Roelofs, 2025, p. 15-7). The third condition is the deliberate continuation of a course of action that is prone to violations, despite the established foundation of knowledge and control. For this reason, the applicability of the doctrine to AWS does not depend on treating the technology as a general instrument, but rather on identifying the individuals and control points directing the process leading to the violation (Üzülmez, 2006, p. 83). Accordingly, the Doctrine of Control over the Organization does not constitute a general solution for responsibility arising from AWS (Orozco López, 2021, p. 233). However, in cases where the control of high-level decision-makers is focused on deployment parameters and risk information is incorporated into the decision-making process in a documented manner, it can serve as a functional instrument for shifting responsibility from the scene of the crime to the decision-making center (Öztürk, 2023, p. 290; Üzülmez, 2006, p. 89). On the other hand, in cases where control is technically and institutionally fragmented, intervention capacity remains limited, or the predictability of system outcomes is low, the implementation of the doctrine may result in problematic extension in terms of the principles of culpability and legality (Öztürk, 2023, p. 292; Tulay, 2019, p. 100). The application of the

concept within the context of AWS must rely on a meticulous framework of attribution that illustrates the distinct parts of control, knowledge, and decision-making.

8.3.2. Organizational Control in ICC Jurisprudence: Indirect Co-Perpetration

In interpreting perpetration under Article 25(3)(a) of the Rome Statute, the ICC adopts the criterion of control over the act. In certain cases, this approach has been further developed through the model of indirect co-perpetration (Lanza, 2018, p. 54; Lee, 2025; Mann, 2019; Ohlin et al., 2013, p. 736; Weigend, 2011, p. 92). The model combines the concept of joint control in co-perpetration with the logic of indirect perpetration through another person. This opens the way for charges under Article 25(3)(a) against high-ranking individuals who, while not present at the scene of the crime, determine the course of action and direct it through an organizational structure (van der Wilt, 2025, p. 632; Weigend, 2011, p. 93). In the line of jurisprudence that began with the Lubanga case and further developed in the Katanga–Chui decisions, the Court does not limit criminal liability solely to the person who commits the act. The determining criterion is the position of control that determines whether a crime will be perpetrated and how it will be committed (Lanza, 2018, p. 24; Shulzhenko & Romashkin, 2021, p. 76; Weigend, 2011, p. 92). In this line of jurisprudence, liability is based on the question of whether the individual made an indispensable contribution to the commission of the crime (Weigend, 2011, p. 110). The court seeks not only the existence of a collective plan but also the concrete manifestation of the contributions that made the plan feasible in practice. Mere general influence, hypothetical authority, or a loose form of coordination is not regarded as sufficient to establish perpetration. This approach makes the question of who established control at what level in multi-party technical structures, such as AWS, the central criterion under Article 25(3)(a) (Kwik, 2023, p. 15). From a comparative legal standpoint, the ICC's methodology incorporates, within a single analytical framework, the control over the act theory of Continental European doctrine and the concept of indirect perpetration via organizational control (van der Wilt, 2025, p. 646; Weigend, 2011, p. 95). Still, it is unfair to automatically equate the concept of organizational dominance with AWS. In fact, this model is based on the assumption that, within a power structure comprising human subordinates, orders are actually carried out and that those who perform them are substitutable (van der Wilt, 2025, p. 644). It is only when certain factual conditions are fulfilled that the system can be regarded as an instrument from an AWS aspect. Indeed, the assessment of organizational control must be treated not as a matter

of the general characteristics of technology, but as a matter of empirical evidence that indicates where control is actually concentrated—whether in the hands of specific individuals or at certain tiers of decision-making (Lanza, 2018, p. 272).

When discussing the responsibility of high-level actors in the context of AWS, the liability for aiding or facilitating under Article 25(3)(c) of the Rome Statute also comes into place. However, mere knowledge does not suffice for this mode of participation, as the Statute necessitates the existence of an intent to facilitate. The dual-use nature of software and system development frequently complicates the ability to definitively demonstrate intent to facilitate a particular war crime. It also underscores the debate in Anglo-American law over whether the standard of "knowledge" or "intent" should be applied to the mental element of liability for participation (Aksenova, 2014, p. 3; Capps, 2024, p. 2; Ohlin, 2013, p. 97). Moreover, a similar level of diligence is required under Turkish criminal law doctrine. Liability is not automatically extended to everyone involved in the act. The principles of legality and culpability set clear boundaries, particularly in the context of expansive interpretations. The principle of accessoriness in participation, along with the distinction between perpetration and participation, requires that material control, the nature of the contribution, and the mental nexus be established in concrete terms. This approach is methodologically consistent with the ICC's criteria of control and indispensable contribution (Lanza, 2018, p. 56). In conclusion, indirect co-perpetration opens a path leading to high-level decision-makers in debates on AWS-related liability. However, this path is possible not via conceptual analogies, but through an evidence-based framework that establishes the relationship of control and the indispensable contribution to the execution of the collective plan (Lanza, 2018, p. 272). Furthermore, ethical issues such as the mechanization of life-and-death decisions constitute a distinct area of discussion that requires separate investigation (Güneysu, 2024a, p. 148) at the intersection of technology and law.

8.3.3. Evaluating the Applicability of the Doctrine to Autonomous Weapon Systems

The approach of indirect perpetration through organizational control seeks to classify the high-level decision-maker who holds decisive authority over the commission of the crime as the perpetrator, rather than the direct perpetrator (Ambos, 2009, p. 564). In the Katanga and Ngudjolo Chui case, the ICC grounded its analysis of indirect perpetration under Article 25(3)(a) of the Rome Statute in a doctrinal line influenced by German legal theory, premised on the idea of commission through a hierarchical organization (Badar, 2010, p. 111). This model is based on the assumption of control over another person's will. The

organizational mechanism effectively ensures the execution of orders, hence it is presumed that the individual at the top executes the acts of others as though they were their own (Weigend, 2011, p. 93). This is where the fundamental issue arises from the AWS perspective, because the machine lacks free will. Therefore, it is not possible to apply the concept of control over one's will in the same way. In Turkish criminal law doctrine, indirect perpetration is generally defined as being perpetrated through a person who lacks the capacity for culpability or over whose free will control has been established (Üzülmez, 2006, p. 91). In the context of AWS, however, the structure cannot be explained through an intermediary person, but only, at most, through an instrument or means employed in the execution of the act (Öztürk, 2023, p. 289). Accordingly, the implementation of organizational control over AWS should not be based on the assumption of control over the will, but rather on the principle of control over actions, which illustrates the actual concentration of control regarding deployment configurations and intervention capabilities.

The second problem stems from the structure of the theory, which is based on the assumptions of the automatic execution of orders and the ease of substitutability. The organizational control approach envisions a mechanism that prevents individual-level disruptions in the execution of orders through a rule-based system (Orozco López, 2021, p. 244; Üzülmez, 2006, p. 90). This mechanism improves the predictability and reliability of the action's execution from the perspective of those in charge. In AWSs, however, the process between sensor data processing and output generation often remains opaque, particularly in complex and dynamic operational environments (Kakko, 2022, p. 12). The absence of transparency and the system's heightened sensitivity to context render the distinction between legitimate and unlawful targeting blurry in practice. In a setting characterized by uncertainty, the presumption of organizational automaticity is diminished. It is no longer straightforward to ascertain that a result will necessarily ensue from the sequence of an action. This situation calls into question both the claim of control over the act and the assessment of responsibility derived from that assumption.

The third, and frequently essential, issue pertains to the establishment of the mental element and its proof. Broadening the scope of indirect perpetration via an organization does not always provide a more consistent basis for the criminal response afforded by existing forms of participation, such as ordering, instigating, and aiding (Weigend, 2011, p. 105). On the contrary, this expansion may blur the boundaries of attribution. By eroding the scope of the concept, it may weaken certainty and predictability (Weigend, 2011, p. 107). This risk is even more apparent in regard to AWS. Unless it is determined which decisions led to a specific violation, what risk information was available, and what intervention

options existed, it becomes difficult to attribute perpetrator status to high-level figures. In this case, attribution becomes controversial in terms of the boundaries drawn by the principle of culpability (Kwik, 2023, p. 25). The critical factors include the system's capabilities and constraints, the usage conditions, the testing and update protocols, and the evidence underlying authorization choices (van den Bosch & Roelofs, 2025, p. 15-6). In other words, the key point is which records can be used to trace the control and risk information.

In conclusion, the organizational control approach does not serve as a solution that automatically and on its own resolves the accountability gap stemming from AWS (Lee, 2025). On the other hand, it offers the possibility of a profound evaluation when targeting high-level actors in situations where control and risk information are highly concentrated, and where concrete evidence demonstrates that a deployment conducive to violations is knowingly and deliberately chosen. In our view, if such factual concentration cannot be demonstrated, the scope of the approach becomes easily ambiguous. Broader and more adaptable practices undermine the explanatory power of the notion by straining both conceptual consistency and the framework of evidence and validation (Orozco López, 2021, p. 237).

8.4. Future Directions in the Light of Normative Gaps and Ethical Considerations

The issue of individual criminal liability in conjunction with AWS is not merely a technical dispute that can be resolved through the interpretation of existing norms. This is because the shift in decision-making regarding the use of lethal force from human will to algorithmic processes simultaneously calls into question the logic of attribution, the principle of culpability, and accountability (Coco, 2023, p. 1079). Even if the ICC's applicability to AWS is accepted in principle, it is argued that the current regime does not sufficiently address the risks specific to these systems (Kalmanovitz, 2016, p. 191). Unpredictability, opacity, and the diminishing role of human control are undermining control and accountability mechanisms (Kwik, 2023, p. 15). Thus, it is emphasized that there is a need for new rules that combine elements of prohibition and strict regulation and, in particular, establish binding multilateral constraints.

Within this framework, three fundamental normative gaps become apparent. The first is the absence of a consistent method for allocating responsibility among developers, manufacturers, suppliers, management, and operators in a supply-and-use chain involving a large number of participants (Guo, 2025, p. 29). Second, within the framework of the Rome Statute, the criteria of knowledge and intent—which occupy a pivotal position—make it difficult in many cases

to establish the mental element through evidence in these systems, which are context-sensitive and can behave in ways that are partially unpredictable (Kwik, 2023, p. 15). Third, despite the normative value of the concept of meaningful human control, it has not yet been turned into a definitive and verifiable set of standards. This situation leaves states with a broad margin for interpretation and delays the establishment of a common framework for practice (Güneysu, 2024b, p. 406). The fundamental ethical objection is that decisions regarding life and death are being detached from human judgment and delegated to systems that operate without human intervention in the targeting and use of force. This situation is inconsistent with human dignity (Ayrancı, 2022). The fact that decisions regarding life and death are based on algorithmic outputs creates uncertainty regarding which individual should bear moral responsibility and on what legal grounds (Lee, 2025). This raises the possibility that responsibility could be distributed throughout the decision-making hierarchy, rather than being attributed to a specific perpetrator.

The UN Secretary-General's statement that systems permitting the taking of life without human intervention are politically unacceptable and morally repugnant indicates that this concern has also found strong resonance at the international institutional level (Bode & Huelss, 2022, p. 4). This shows that the issue is not merely a technical discussion of risk; it is also a matter of boundaries in terms of normative legitimacy and human dignity. The demand for the establishment of a binding international instrument by 2026 indicates that the necessity for regulation has transcended beyond doctrinal debate (Monnett, 2024, p. 15). For this reason, the issue is not a procedural problem that can be resolved by interpreting the existing rules. It is an area that requires urgent action at the policy-making level. The Group of Governmental Experts within the CCW continues discussions on a clear divergence in approach regarding policy and security (Bode & Huelss, 2022, p. 35). One side advocates for the establishment of new and binding rules for AWS, while the other argues that the issue can be managed using the instruments and principles of the existing international humanitarian law regime (Bode & Huelss, 2022, p. 38). Nevertheless, a growing body of literature points to a dual regulatory model. Under this model, systems that are structurally incapable of complying with international humanitarian law are prohibited. In systems where compliant use is theoretically feasible, strict guidelines and positive obligations are instituted to guarantee compatibility throughout the entire design, testing, procurement, and deployment process (Guo, 2025, p. 37; Monnett, 2024, p. 15). The key elements of this approach include making weapons review an institutional requirement, narrowing the categories of targets, strictly limiting the use of weapons in terms of time and location, strengthening operator qualifications, and mandating the maintenance of operational records.

From a criminal law perspective, what is determinative in each specific case is who holds the authority to exercise control and which institutional records can be used to track risk information (Massingham & McKenzie, 2021, p. 177). The principles of culpability, legality, and certainty do not permit the attribution of perpetrator status to an individual solely on the basis of the occurrence of the result. Therefore, criminal liability can be legally justified only to the extent that a concrete link can be established between knowledge of the risk, the ability to exercise actual control, authorization, and the choice of deployment (Kwik, 2023, p. 18). Similarly, under Turkish criminal law, the differentiation between perpetration and participation necessitates the tangible establishment of both material control over the crime and the mental nexus of participation (Demirel & Kartal, 2019, p. 480). These circumstances remove the evaluation from hypothetical assumptions while directing the examination toward the factual evidence of the incident. In other words, the decisive factors become the questions of who possesses what information and which means of intervention can be utilized. Consequently, the emphasis of the debate is not on normative characterizations. The essential factor is the evidence available to establish a chain of inference in the specific situation.

The Foreseeability and Control (FC) test, documented in the literature as a practical normative instrument linking meaningful human control to criminal culpability, is proposed (Kersten, 2025). The FC test does not narrow the examination of control down to a single moment of decision. It spreads the assessment across the design, testing, procurement, training, deployment, and update phases. In this way, the institutional traces of control and knowledge of risk are examined in a holistic manner (Jain, 2016, p. 166). The concept is founded on five analytical domains. First, the chain of authority and decision-making must be transparent; it must be possible to trace who determines critical parameters. Second, predictability and explainability are essential; system faults must be anticipated, and outputs must be verifiable. Third, contextual risk intensity necessitates the implementation of stricter human monitoring in high-risk contexts. Fourth, verification and logging records; test and operational data must be accessible. Fifth, the system must possess intervention and shutdown capabilities, allowing it to be shut down when necessary. In our view, the FC test can be adapted to serve as a more restrictive attribution formula in criminal law. According to this formula, the individual must possess information from organizational documents on the risk of an IHL violation in the pertinent operational context, or be anticipated to have access to such information (Kwik, 2023, p. 11). If the individual continues the deployment despite having the ability to restrict or intervene in the system, or fails to implement mandatory restrictions, the choice to use the system in a

violation-prone manner is attributed to the individual. In this case, the result cannot be treated as an autonomous output of the system. The outcome can be normatively attributed to the individual based on the deliberate taking of a risk within their area of responsibility or the failure to mitigate such a risk through negligence. This strict formula elucidates the debate over the knowledge element under Article 30 of the Rome Statute, removing it from the realm of ambiguity. It shifts the discussion to a risk-awareness framework based on records. It also renders the duty to prevent under command responsibility assessable on the basis of concrete evidence (Guo, 2025, p. 35; Massingham & McKenzie, 2021). The concept of strict liability is sometimes proposed as a way to overcome the impasse regarding the mental element. However, this approach is incompatible with the structure of international criminal law, which is based on individual culpability (Coco, 2023, p. 1095; Kwik, 2023, p. 23). Separating criminal responsibility from the elements of knowledge and intent weakens legal certainty and foreseeability under the principle of legality. In contrast, internalizing risk at the organizational level through administrative sanctions, procurement and contractual mechanisms, product safety obligations, and liability for damages offers a more functional solution (Kalmanovitz, 2016, p. 192). This approach establishes preventive compliance measures and effective accountability mechanisms for the development and utilization of high-risk technologies without pushing the boundaries of criminal law.

The practical recommendations for Türkiye aim to establish institutional counterparts at the national level for the international approach (Güneysu, 2023, p. 97). Accordingly, independent technical and legal assessments should be required at the procurement and deployment stages. Moreover, keeping records related to system usage must be standardized and retained (Kersten, 2025). Furthermore, limitations related to the scope of duties must be documented. These constraints must be authorized in a traceable manner within the chain of command and subjected to regular oversight (Kersten, 2025). Decisions regarding operator training and authorization should also be subject to the documentation requirements. These documents must clearly outline the risk assessment and operating parameters (Kwik, 2023, p. 26). Additionally, parliamentary oversight and administrative supervision must be strengthened, as such an institutional structure removes attribution in criminal law from reliance on assumptions. It also makes the relationship among knowledge, control capacity, and choice visible through concrete evidence. In this way, while the principle of culpability is preserved, the possibility of impunity is minimized (Coco, 2023, p. 1096; Kersten, 2025). The proposed model is not a solution that closes the liability gap in a single step. Nonetheless, it makes it methodologically possible to focus on high-level actors in cases where control

and risk information are concentrated at higher levels. Therefore, it must be shown that a deployment conducive to violations was knowingly preferred or that the requisite limitations were consciously not implemented (Kwik, 2023, p. 18). Failing this, expansive and imprecise applications disproportionately widen the scope of attribution, compromising both theoretical consistency and the evidentiary framework. This undermines both theoretical consistency and the structure of the proof (Weigend, 2011, p. 107). Therefore, in our opinion, the focus of the discussion should be on the concrete system of evidence that can be established via the chain of command and risk trails.

8.5. Conclusion

The issue of culpability in AWS does not stem from the debate over whether machines can be legally held responsible. The issue stems from the distribution of the decision to employ lethal force throughout the design, testing, procurement, training, deployment, and update phases, resulting in diminished transparency in the decision-making processes. Therefore, the critical factor is not the theoretical applicability of international humanitarian law, but the ability to demonstrate, on a case-by-case basis and supported by evidence, who possesses information regarding the risk of a violation and where the authority to exercise control and intervene is genuinely concentrated. The structures of the Rome Statute relating to perpetration, participation, and command responsibility are not entirely inoperative. However, the review of responsibility should focus more on those who define the mission parameters and have the actual ability to restrict the system, rather than on the physical operator in the field. This is because criminal law liability is not based solely on the occurrence of the result. Attribution is based on the connection between the authority to control, knowledge of the risk, and the choice made despite that awareness.

While the current mechanisms are theoretically relevant, establishing culpability in AWS cases relies on the criteria of joint control and indispensable contribution. In this regard, it must be demonstrated in a documented manner who holds the risk information, what records are available, and under what authority and with what approval decisions are made. Otherwise, attribution becomes diffused within legal ambiguity. In this regard, the implementation of the ICC's "knowledge and intent" standard requires that predictability be concretized through institutional records such as warnings, test results, field records, and update histories. With regard to command responsibility, effective control cannot be reduced solely to the authority to issue orders to personnel. Effective control also includes actual authority over the engagement threshold, the target pool, geographical and temporal constraints, cancellation protocols, human oversight, and the record keeping. Lastly, concerns surrounding the use of

lethal force do not constitute a factor that alleviates the duty of diligence. On the contrary, it necessitates the establishment of stricter and more verifiable planning and operational oversight standards. Within the framework of AWS, suggestions for strict liability seem justifiable due to the challenges associated with establishing the mental element. However, a model that excludes the elements of knowledge and intent is incompatible with the structure of international criminal law, which is based on individual culpability. Furthermore, it carries the risk of an expansion that is difficult to defend on legitimacy, certainty, and predictability grounds. In our view, a more appropriate solution is to internalize system-related risks at the organizational level through administrative sanctions, procurement and contractual mechanisms, product safety obligations, and compensation regimes. Criminal culpability should, in turn, be limited to cases where documented knowledge of risk and actual control capacity are concentrated. Within this framework, liability should be established when the decision to deploy or sustain the system is made deliberately. In this way, both theoretical compliance is maintained, and the scope of impunity is narrowed.

In our view, a two-tier regulatory model offers a minimum common ground for consensus. According to this model, systems that are not consistent with humanitarian law should be explicitly prohibited. For other systems, binding obligations—such as weapons reviews, transparency and traceability, record-keeping, and the capacity for effective intervention—should be established throughout their lifecycle. This approach facilitates the establishment of a common normative basis grounded in accountability, even if divisions of opinion persist in the CCW/GGE discussions. This is because removing lethal decision-making from human judgment creates an ethical dilemma that undermines human dignity. Along with that, it erodes transparency by making it unclear who should be held accountable, on what grounds, and based on what information. Therefore, the need for a binding international regulation is no longer merely a theoretical debate. It is gaining prominence in discussions on direct norm-setting. Finally, under Turkish criminal law concerning the principles of culpability and legality, the mere occurrence of a result is not sufficient to establish the status of a perpetrator. Attribution cannot be determined without an evidentiary demonstration, in each specific case, of control over the act and the mental element required by the distinction between perpetration and participation. Indeed, in AWS cases, it is not the abstract assessment of the technology that is decisive. A definitive framework for attribution relies on record traceability, the chain of command, and evidence pertaining to risk awareness.

References

Aksenova, M. (2014). *Returning to complicity for core international crimes* (Policy Brief No. 17). TOAEP. https://www.legal-tools.org/doc/15a3a4/

Ambos, K. (2009). Politische und rechtliche Hintergründe des Urteils gegen den ehem peruanischen Präsidenten Alberto Fujimori. *Zeitschrift für Internationale Strafrechtsdogmatik,* (11), 552–564. https://www.zis-online.com/dat/artikel/2009_11_368.pdf

Asaro, P. M. (2025). *Regulating autonomous weapons: Recent diplomatic & political developments* [Conference presentation]. 63rd ISODARCO Course. https://www.isodarco.it/wp-content/uploads/2025/10/asaro_paper_63rd-isodarco-course.pdf

Australia, Canada, Japan, Republic of Korea, United Kingdom, & United States. (2021, September 27). *Building on Chile's proposed four elements of further work for the Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts (GGE) on emerging technologies in the area of lethal autonomous weapons systems (LAWS)* (CCW/GGE.1/2021/WP.2). United Nations. https://docs.un.org/en/CCW/GGE.1/2021/WP.2

Ayrancı, A. K. (2022). *Uluslararası deniz hukuku uyarınca otonom deniz araçları statüsünün incelenmesi ve denizde silahlı çatışma hukuku kapsamında otonom deniz silah sistemlerinin kullanımının değerlendirilmesi*. Yetkin Yayınları.

Badar, M. E. (2010). Some reflections on Article 30 of the Rome Statute in light of the Lubanga & Katanga decisions on the confirmation of charges. In O. Triffterer, C. Vogel, & C. Burchard (Eds.), *The review conference and the future of the International Criminal Court* (pp. 109–130). Kluwer Law International.

Bauer, R. (2016). *Organisationsherrschaft in Wirtschaftsunternehmen* [Doctoral dissertation, Bucerius Law School].

Bo, M., Bruun, L., & Boulanin, V. (2022, October). *Retaining human responsibility in the development and use of autonomous weapon systems: On accountability for violations of international humanitarian law involving AWS*. Stockholm International Peace Research Institute.

Bode, I., & Huelss, H. (2022). *Autonomous weapons systems and international norms*. McGill-Queen's University Press.

Boulanin, V. (2016). Mapping the development of autonomy in the military sphere. In R. Geiß (Ed.), *Lethal autonomous weapons systems: Technology, definition, ethics, law & security* (pp. 26–35). German Federal Foreign Office.

Campani Farias, L. (2025). GGE on LAWS rolling text: Strengthening human control operationalization. *IA Policy Brief Series, 7*(1), 1–5. https://doi.org/10.5281/zenodo.16416661

Capps, C. F. (2024). Rethinking accomplice liability. *Arizona State Law Journal, 56*, 1–52

Chaitidou, E. (2016). Recent developments in the jurisprudence of the International Criminal Court. *Zeitschrift für Internationale Strafrechtsdogmatik,* (12), 813–850. https://www.zis-online.com/dat/artikel/2016_12_1072.pdf

Coco, A. (2023). Exploring the impact of automation bias and complacency on individual criminal responsibility for war crimes. *Journal of International Criminal Justice, 21*(5), 1077–1096. https://doi.org/10.1093/jicj/mqad034

Dahlmann, A. (2016). Getting a grasp of LAWS? What quantitative indicator-based approaches could bring to the debate. In R. Geiß (Ed.), *Lethal autonomous weapons systems: Technology, definition, ethics, law & security* (pp. 36–43). German Federal Foreign Office.

Demirel, M., & Kartal, M. (2019). Ceza hukukunda suça azmettirme hareketi: Suça sevk etme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 21*(2), 457–490.

Frunzeti, T., Tomoiagă, T., & Coşereanu, L. (2025). Challenges that new technologies are bringing in future defence planning and military operations. *Annals Academy of Romanian Scientists Series on Military Sciences, 17*(3), 3–17. https://doi.org/10.56082/annalsarscimilit.2025.3.3

Geiß, R. (2016). Autonomous weapons systems: Risk management and state responsibility. In R. Geiß (Ed.), *Lethal autonomous weapons systems: Technology, definition, ethics, law & security* (pp. 109–118). German Federal Foreign Office.

Gjorgjinski, L. (2021, April 19). *Chairperson's summary* (CCW/GGE.1/2020/WP.7). United Nations. https://docs.un.org/en/CCW/GGE.1/2020/WP.7

Greipl, A. R. (2023). Data-driven learning systems and the commission of international crimes: Concerns for criminal responsibility? *Journal of International Criminal Justice, 21*(5), 1097–1118. https://doi.org/10.1093/jicj/mqad031

Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. (2017, December 22). *Report of the 2017 Group of Governmental Experts on lethal autonomous weapons systems (LAWS)* (CCW/GGE.1/2017/3). United Nations. https://docs.un.org/en/CCW/GGE.1/2017/3

Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. (2022, February 22). *Report of the 2021 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems* (CCW/GGE.1/2021/3). United Nations. https://docs.un.org/en/CCW/GGE.1/2021/3

Güneysu, G. (2023). Yeni silahların tabi tutulması gereken hukukîlik denetimi ve otonom silah sistemleri. *Düşünce Dünyasında Türkiz, 14*, 81–105. https://doi.org/10.59281/turkiz.1258725

Güneysu, G. (2024a). Autonomous weapon systems and the humanitarian principle of distinction. *Annales de la Faculté de Droit d'Istanbul, 74*, 133–153. https://doi.org/10.26650/annales.2024.74.0007

Güneysu, G. (2024b). Lethal autonomous weapon systems and automation bias. *Yuridika, 39*(3), 395–424. https://doi.org/10.20473/ydk.v39i3.55188

Güneysu, G. (2025). Autonomous weapon systems and international criminal justice: Is deterrence still possible? *The International Journal of Human Rights*, 1–14. https://doi.org/10.1080/13642987.2025.2594775

Guo, J. (2025). The ethical legitimacy of autonomous weapons systems: Reconfiguring war accountability in the age of artificial intelligence. *Ethics & Global Politics, 18*(3), 27–39. https://doi.org/10.1080/16544951.2025.2540131

International Committee of the Red Cross. (2021, May 12). *ICRC position on autonomous weapon systems*. https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems

Jain, N. (2016). Human-machine interaction in terms of various degrees of autonomy as well as political and legal responsibility for actions of autonomous systems. In R. Geiß (Ed.), *Lethal autonomous weapons systems: Technology, definition, ethics, law & security* (pp. 160–170). German Federal Foreign Office.

Jenks, C. (2016). The distraction of full autonomy and the need to refocus the CCW LAWS discussion on critical functions. In R. Geiß (Ed.), *Lethal autonomous weapons systems: Technology, definition, ethics, law & security* (pp. 171–183). German Federal Foreign Office.

Kakko, Y. (2022, January). *Meaningful human control as an exceptional concept: Added value and common ground for CCW discussions on lethal autonomous weapons systems*. SaferGlobe. https://www.nonproliferation.eu/wp-content/uploads/2022/01/KakkoMeaningfulHumanControl2022-1.pdf

Kalmanovitz, P. (2016). Lethal autonomous weapons systems and the risks of "riskless warfare." In R. Geiß (Ed.), *Lethal autonomous weapons systems: Technology, definition, ethics, law & security* (pp. 184–195). German Federal Foreign Office.

Kersten, M. (2025, August 6). *Algorithms, automation and accountability: Imagining responsibility for the crimes of machines*. Justice in Conflict. https://justiceinconflict.org/2025/08/06/algorithms-automation-and-accountability-imagining-responsibility-for-the-crimes-of-machines/

Kwik, J. (2023). The conceptual roots of the criminal responsibility gap in autonomous weapon systems. *Melbourne Journal of International Law, 24*(1), 1–26. https://law.unimelb.edu.au/mjil/issues/issue-archive/241

Lanza, G. (2018). *Indirect perpetration and Organisationsherrschaft: An analysis of Art. 25(3)(a), third alternative, ICCSt taking into account the "German" differentiated model and the "Italian" unitarian model of participation in a crime* [Doctoral dissertation, Università degli Studi di Verona and Georg August University of Göttingen]. IRIS. https://hdl.handle.net/11562/985964

Lee, J. (2025). Autonomous weapons, war crimes, and accountability. *North Carolina Journal of International Law, 49*(2). https://scholarship.law.unc.edu/ncilj/vol49/iss2/4/

Mann, J. K. (2019, July 15). *Autonomous weapons systems and the liability gap, part one: Introduction to autonomous weapons systems and international criminal liability*. Rethinking SLIC. https://www.rethinkingslic.org/blog/criminal-law/51

Massingham, E., & McKenzie, S. (2021). Testing knowledge: Weapons reviews of autonomous weapons systems and the international criminal trial. In E. Palmer, E. Bikundo, S. Harris Rimmer, & M. Clark (Eds.), *Futures of international criminal justice* (pp. 177–197). Routledge. https://doi.org/10.4324/9781003087533-11

Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. (2019, December 13). *Final report* (CCW/MSP/2019/9). United Nations. https://docs.un.org/en/CCW/MSP/2019/9

Monnett, L. (2024, July). *Sending up a flare: Autonomous weapons systems proliferation risks to human rights and international security* [Research brief]. Geneva Academy of International Humanitarian Law and Human Rights. https://geneva-academy.ch/wp-content/uploads/2025/09/Sending-Up-a-Flare-Autonomous-Weapons-Systems-Proliferation-Risks.pdf

Moyes, R. (2016). Meaningful human control. In R. Geiß (Ed.), *Lethal autonomous weapons systems: Technology, definition, ethics, law & security* (pp. 239–249). German Federal Foreign Office.

Ohlin, J. D. (2013). Targeting and the concept of intent. *Michigan Journal of International Law,* 35(1), 79–130.

Ohlin, J. D., van Sliedregt, E., & Weigend, T. (2013). Assessing the control-theory. *Leiden Journal of International Law, 26*(3), 725–746. https://doi.org/10.1017/S0922156513000319

Orozco López, H. D. (2021). Roxins mittelbare Täterschaft kraft organisatorischer Machtapparate: Eine kritische Analyse. *Zeitschrift für Internationale Strafrechtsdogmatik,* (4), 233–248. https://www.zis-online.com/dat/artikel/2021_4_1429.pdf

Öztürk, M. K. (2023). Türk Ceza Kanunu'nda bir iştirak şekli olarak faillik (TCK m. 37). *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, 13*(1), 255–307.

Petersen, J. (2024). Die "neutrale Handlung" im Strafrecht – Eine Untersuchung insbesondere der neutralen Beihilfe. *Zeitschrift für Internationale Strafrechtswissenschaft,* (4), 286–291. https://www.zfistw.de/dat/artikel/2024_4_1623.pdf

Petrović, P., Dias, M. T. M., Grasso, N., Botella Berenguer, V. V., & Denieul, M. (2024, November). *The role of AI decision-making for land-based operations*. FINABEL

Renzikowski, J. (2021). Die fahrlässige Mittäterschaft. *Zeitschrift für Internationale Strafrechtsdogmatik, 16*, 92–99. https://www.zis-online.com/dat/artikel/2021_2_1416.pdf

Rotsch, T. (2009). Von Eichmann bis Fujimori – Zur Rezeption der Organisationsherrschaft nach dem Urteil des Obersten Strafgerichtshofs Perus. *Zeitschrift für Internationale Strafrechtsdogmatik,* (11), 549–551. https://www.zis-online.com/dat/artikel/2009_11_367.pdf

Roxin, C. (2006). Organisationsherrschaft und Tatentschlossenheit. *Zeitschrift für Internationale Strafrechtsdogmatik,* (7), 293–300. https://www.zis-online.com/dat/artikel/2006_7_44.pdf

Schünemann, B. (2006). Die Rechtsfigur des „Täters hinter dem Täter" und das Prinzip der Tatherrschaftsstufen. *Zeitschrift für Internationale Strafrechtsdogmatik,* (7), 301–308. https://www.zis-online.com/dat/artikel/2006_7_45.pdf

Shulzhenko, N., & Romashkin, S. (2021). Types of individual criminal responsibility according to Article 25(3) of the Rome Statute. *Juridical Tribune – Review of Comparative and International Law, 11*(1), 72–80.

Suchman, L. (2016). Situational awareness and adherence to the principle of distinction as a necessary condition for lawful autonomy. In R. Geiß (Ed.), *Lethal autonomous weapons systems: Technology, definition, ethics, law & security* (pp. 273–283). German Federal Foreign Office.

Tezcan, D., Erdem, M. R., & Önok, R. M. (2023). *Uluslararası ceza hukuku* (7. baskı). Seçkin Yayıncılık.

Tulay, M. E. (2019). Suç örgütü liderinin cezai sorumluluğuna ilişkin hukuki analiz ve öneriler (TCK m. 220/5). *Türkiye Adalet Akademisi Dergisi,* (38), 89–106. https://dergipark.org.tr/tr/pub/taad/article/549062

Üzülmez, İ. (2006). Dolaylı faillik (TCK m. 37/2). *Erciyes Üniversitesi Hukuk Fakültesi Dergisi,* 1(2), 79–95. https://dergipark.org.tr/en/pub/eruhfd/article/1564130

van den Bosch, K., & Roelofs, M. (2025). *Intelligent decision support and meaningful human control in multi-domain operations* (STO-MP-HFM-377). NATO Science and Technology Organization.

van der Wilt, H. (2025). Leadership responsibility in non-state criminal organisations: The rediscovery of indirect perpetration through an organisation by Latin American courts and the ICC. *The International Journal of Human Rights, 29*(4), 632–649. https://doi.org/10.1080/13642987.2024.2357137

Weigend, T. (2011). Perpetration through an organization: The unexpected career of a German legal concept. *Journal of International Criminal Justice, 9*(1), 91–111. https://doi.org/10.1093/jicj/mqq077

Westhues, A. H. (2025). The militarization of artificial intelligence and the autonomous weapons. *UNISCI Journal,* (67), 111–136. https://doi.org/10.31439/UNISCI-222