Scientific and Social Research, 2025, Volume 7, Issue 12
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Autonomous Weapon Systems and Individual Criminal Liability under the Rome Statute

Zhaohang Tong*

The University of Western Australia, Perth 6009, Australia

Abstract: Autonomous weapon systems (AWS) pose significant challenges for individual criminal responsibility under the Rome Statute. While existing modes of liability—such as perpetration, ordering, aiding and abetting, and command responsibility—can theoretically apply to AWS-related crimes, their effectiveness depends on human intent and control. When autonomous systems act unpredictably, attribution of the actus reus, mens rea, and causation becomes uncertain, creating a "responsibility gap" in which no human perpetrator can be clearly identified. This paper evaluates how the International Criminal Court could adapt existing doctrines to address this gap, including broader interpretations of perpetration-by-means, omission liability, and expanded command responsibility. It also assesses proposals for new offences, prosecutorial guidelines, and non-criminal accountability mechanisms. The analysis argues that legal innovation is essential to ensure that accountability remains human-centred as warfare becomes increasingly automated.

Keywords: Autonomous weapon systems (AWS); Rome Statute; Individual criminal responsibility; Actus reus; Mens rea; Command responsibility; Responsibility gap

Online publication: December 31, 2025

1. Introduction

Autonomous weapon systems (AWS) are weapons that can select and attack targets without meaningful human control. These technologies are transforming warfare but also creating serious legal questions about accountability when civilians are unlawfully killed.[1-2] As scholars note, outcomes in AI systems emerge from a web of "human, physical, and computational" interactions, making it difficult to identify a single responsible actor.[3-5] This complexity lies at the heart of the modern "responsibility gap", where serious harm may occur but no individual can be clearly blamed.[3-5] Under the Rome Statute of the International Criminal Court (ICC), "only natural persons can be prosecuted for crimes such as war crimes or crimes against humanity."[6] Machines have no consciousness or intent, which further complicates attribution when an autonomous system causes unlawful harm.[3-5] If a robot or drone kills civilians, who can be held criminally liable—the operator, the commander, the programmer, or no one at all?

This paper examines how individual criminal responsibility can be established under the Rome Statute when

war crimes or crimes against humanity are committed through AWS. It explores the modes of liability that may apply, the obstacles in proving the guilty act, the guilty mind, and causation, and it discusses possible doctrinal solutions for ensuring accountability.[7-12] The analysis remains focused on international criminal law (ICL) rather than the legality of AWS under international humanitarian law (IHL).[8-10] The aim is to assess how ICL can adapt to technological change while upholding justice for victims of autonomous warfare.[1-5,7-12]

2. AWS and International Crimes under the Rome Statute

AWS include armed drones with artificial intelligence, automated sentry guns, and future robotic soldiers capable of independent targeting.[7,26] If such systems cause unlawful deaths or destruction, they may fall within existing international crimes defined in the Rome Statute.

War crimes may arise if an AWS deliberately or indiscriminately attacks civilians, hospitals, or other protected persons.[6,7,10] Article 8 of the Rome Statute covers acts such as "intentionally directing attacks against the civilian population" or "launching an indiscriminate attack" likely to cause excessive civilian harm.[6] Crimes against humanity may also be committed where AWS are used as part of a widespread or systematic attack on civilians — for example, if a government uses autonomous drones to suppress protests or target an ethnic minority. In such cases, crimes like murder or persecution under Article 7 may apply.[6,11]

However, the ICC recognises only individual criminal responsibility. Article 25(1) confirms that the Court has jurisdiction solely over natural persons.[6] Any harm caused by AWS must therefore be attributed to a human perpetrator. The Rome Statute offers several modes of liability — direct or indirect commission, ordering, aiding and abetting, and command responsibility under Article 28.[6,11,13,28] These provisions provide the foundation for accountability, but applying them to machines introduces new complexity. The challenge is to fit the actions of autonomous systems into doctrines built on human conduct and intention.

3. Modes of Liability for AWS — Related Crimes

3.1. Direct Perpetration and Perpetration-by-Means

The most direct way to establish liability is to treat the human who deploys or controls an autonomous weapon as the perpetrator. Under Article 25(3)(a) of the Rome Statute, a person "commits" a crime either directly or "through another person."[6,13] Traditionally, perpetration-by-means applies when someone uses an innocent agent — such as a coerced or mentally incapacitated person — to commit an offence.[11-13] By analogy, an AWS can be seen as an innocent instrument, as it operates without independent will or moral agency.[3-5,11-13] Thus, if a commander programs or instructs an AWS to strike civilian objects, the commander is the true perpetrator, and the machine merely executes the physical act.

However, this reasoning works only where the human retains control and intent. Many AWS act independently after activation, making unpredictable targeting choices.[3-5,20] If a system takes an unforeseen lethal decision, it becomes difficult to say that the human "committed" that specific act. Perpetration-by-means therefore fits only when the human intentionally uses an AWS for an unlawful purpose — such as deploying a weapon known to be indiscriminate — but not when the outcome results from autonomous malfunction or error.[3-5,7,20]

3.2. Ordering, Aiding and Abetting

Responsibility for war crimes can arise in different ways under the Rome Statute. Under Article 25(3)(b), a person

who orders the commission of a crime is responsible as if they had committed it themselves.[6,14] Therefore, a commander who instructs subordinates to employ an AWS in a populated area may be guilty of ordering any resulting war crimes.[14] In contrast, Article 25(3)(c) covers aiding and abetting, which applies when a person intentionally assists or facilitates the commission of a crime.[6,15] A software engineer or contractor who designs targeting algorithms knowing that they will select prohibited targets provides such assistance and could be liable as an aider and abettor.[3-5,12,15] Although proving this knowledge is difficult, it shows that liability can extend beyond direct operators to those involved in developing or supplying AWS.[3-5,11-12]

Under Article 25(3)(d) of the Rome Statute, a person may be responsible for war crimes if they intentionally contribute to a group activity that aims to commit such crimes.[6,16] This approach is similar to the "joint criminal enterprise" doctrine developed by the ICTY in Prosecutor v Tadić, where collective intent and coordinated participation were found sufficient for liability.[17-18] Applying this model, networks of military officials and engineers who knowingly collaborate in deploying AWS for unlawful attacks could share responsibility for the resulting crimes, recognising that modern weapon systems are products of collective design and decision-making rather than the acts of one person alone.[3-5,11-12,19-20]

3.3. Command Responsibility

Article 28 establishes "command or superior responsibility, holding military leaders accountable for crimes committed by their subordinates when they knew or should have known of the offences and failed to prevent or punish them".[6,11,28] This doctrine, however, assumes a human subordinate capable of intent. An AWS, however advanced, cannot be a legal subordinate — it has no will or mens rea.[19,20] As Alessandra Spadaro notes, "a weapon is no subordinate".[19] A commander who deploys an AWS that commits atrocities may therefore escape direct liability under Article 28 because no human subordinate carried out the attack.

Nonetheless, if human teams are involved in programming, launching, or supervising the AWS, the commander can still be liable for failing to control those subordinates. Scholars have proposed expanding command responsibility to include a duty to control weapons systems, ensuring that commanders remain accountable for the conduct of the technology they employ.[5,19-21]

3.4. Omission Liability

A final possible mode is liability by omission — failure to act when under a legal duty to intervene.[22,28] Under general principles and Article 86 of Additional Protocol I, those who plan or execute attacks must take precautions and cancel unlawful strikes.[22-23] An AWS operator who observes that the system is attacking civilians but fails to stop it may therefore be criminally responsible. Although the Rome Statute does not expressly equate omissions with acts, international tribunals such as the ICTY and ICTR have recognised that a failure to act can incur criminal responsibility where a person had both the duty and the ability to prevent the crime.[5,22,24-25] Recognising omission liability would help close the gap in cases where humans could have prevented an AWS's unlawful attack but chose not to intervene.[3-5,22,24-25]

3.5. Obstacles in Assigning Liability

Although the Rome Statute provides several modes of liability, applying them to crimes involving autonomous weapon systems (AWS) faces major difficulties.[3-6,11,28] The main challenges concern the actus reus, the mens rea, and the causal link between human actions and the outcome. These issues create what scholars call a "responsibility

gap", where serious harm occurs but no individual can be legally blamed.[3-5]

3.5.1. Actus Reus and Attribution

In international criminal law, a perpetrator must perform a prohibited act, such as killing or attacking civilians, or fail to act despite a legal duty.[11,28] In AWS cases, however, the lethal act — pressing the trigger or choosing a target — is done by the machine, not the human.[3,19-20] Caton argue that a commander's decision to deploy an AWS could itself constitute the actus reus, especially if done in a civilian area with knowledge of likely harm.[26] Yet this interpretation stretches the legal concept of "directing an attack". Article 8 offences, such as "intentionally directing attacks against civilians", assume a person chose specific victims.[6,20] f an AWS independently selects and attacks targets, attributing that conduct to a human becomes problematic, because autonomous operation removes direct human control and intent, making it difficult to satisfy the actus reus and mens rea elements required for individual liability.[3-5,20]

Causation is equally complex. AWS operate through algorithms and sensors that can malfunction or act unpredictably.[3-5,7] A defence lawyer might argue that the autonomous system's decision was an intervening cause — breaking the causal link between human conduct and the unlawful result.[11,28] Because autonomous operations depend on a network of human inputs, physical components, and computational processes, determining who or what actually caused the outcome becomes highly uncertain.[3-5,20,28] The more autonomous the system, the weaker the causal connection to the human who deployed it, challenging traditional understandings of criminal conduct.[3-5,20]

3.5.2. Mens Rea

The Rome Statute generally requires crimes to be committed with intent and knowledge, as is standard in criminal law.[6,27,28] However, establishing these mental elements becomes difficult when actions are carried out by autonomous systems operating without human awareness or direct control.[3-5,19-20] To understand this difficulty, it is necessary to recall how the Statute defines intent and knowledge. A person acts intentionally if they mean to engage in the conduct and cause the consequence, or if they know the consequence will occur "in the ordinary course of events".[6,27] This covers direct and oblique intent but not lower mental states like recklessness or negligence, except in specific provisions such as command responsibility.[6,11,27]

Applying this to AWS creates two distinct scenarios. In cases of intentional misuse, such as deliberately programming an AWS to target civilians, the perpetrator's intent is clear, and liability under Article 25(3)(a) of the Rome Statute can apply.[3,6,13,26] However, in unintended incidents, where an AWS malfunctions or misidentifies a target, the operator's state of mind may amount only to recklessness or negligence. Because Article 30 excludes recklessness, such individuals may escape liability.[6,27,28] Accidental targeting errors in war are rarely prosecuted as war crimes, and AWS — related incidents might similarly fall outside criminal responsibility.[1,3,5,20]

This mental gap is central to the accountability problem. Human Rights Watch warns that many AWS cases would "elude justice" because humans could neither foresee nor prevent the system's actions.[1] Without intent or clear control, both actus reus and mens rea fail, leaving victims without a responsible perpetrator.[1,3-5]

3.5.3. Diffuse Responsibility and the "Many Hands" Problem

AWS also complicate responsibility through the involvement of multiple actors — commanders, operators, engineers, and manufacturers.[3-5,11,19-20] Each contributes in part, but none alone determines the final unlawful act. This diffusion of responsibility, sometimes called the "problem of many hands", makes it difficult to identify a

single guilty mind.[3-5] As scholars observe, modern targeting involves layered decisions in which each participant can claim reliance on others or on the system itself.[3-5,19-20] The result is systemic accountability failure: civilians may die, but everyone involved can plausibly deny blame.[1,3-5]

Overall, the combination of unclear causation, limited mens rea standards, and dispersed control means that current doctrines struggle to capture AWS-related crimes. Unless international law evolves to recognise shared or indirect responsibility, the "responsibility gap" will persist—allowing grave violations to go unpunished.[1,3-5,19-20,28]

4. Possible Doctrinal Solutions and the Way Forward

Addressing the challenges of autonomous weapon systems (AWS) under the Rome Statute requires both creative interpretation and potential legal development.[1,3-6,11,19-20] Scholars and policy experts have proposed several ways to close the accountability gap and ensure that human responsibility remains central even in an age of automation.[1-5,11,19-20] The following section analyses these proposed approaches, evaluating how each could operate within the framework of international criminal law and the Rome Statute.

4.1. Broadening Interpretation of Existing Provisions

One pragmatic solution is to interpret existing provisions of the *Rome Statute* more flexibly. Article 25(3)(a) already allows crimes to be committed "through another person", even if that person is not criminally responsible.[6,13] By analogy, an autonomous system could be treated as a non — responsible agent, much like an innocent intermediary.[3-5,11-13,19-20] The human who programs, deploys, or directs the AWS would thus remain the principal perpetrator. This interpretation ensures that the absence of machine intent does not block human accountability.[3-5,11-13,19-20]

Courts could also recognise commission by omission. Even though the Statute does not expressly equate omissions with acts, judges could draw from both general principles of law and Article 86 of Additional Protocol I, which obliges states to prevent violations.[22-23] Under this reasoning, if a commander or operator fails to stop an unlawful AWS attack despite having both the duty and capacity to act, their inaction could satisfy the actus reus of the crime.[22,24-25] This approach would shift focus from what the machine did to what the human failed to prevent.[3-5,11,22,24-25]

Another interpretive adjustment concerns mens rea. While Article 30 of the Rome Statute requires intent and knowledge, international jurisprudence could evolve to recognise dolus eventualis — awareness of a high risk and acceptance of that risk — as sufficient intent.[6,27-28] If a commander deploys an AWS knowing that civilian deaths are highly probable, such willful blindness could meet the intent standard.[6,11,27-28] Some ICTY judgments on indiscriminate shelling have already treated reckless indifference as enough to establish intent. The ICC could adopt a similar reasoning to cover cases involving inherently dangerous AWS.[24-25,27-28]

4.2. Expanding Command Responsibility

Because current command responsibility under Article 28 of the Rome Statute assumes human subordinates, it does not fit well when the "actor" is a machine.[6,11,19-20] A possible reform is to develop a doctrine of "materiel responsibility" — holding commanders accountable for failing to control their weapons systems.[5,19-21] Commanders would be legally obliged to ensure that any AWS under their authority complies with international humanitarian and criminal law. If they deploy a weapon incapable of distinguishing civilians from combatants,

they could be held responsible for the resulting crimes.[3-5,7-8,11,19-21]

This concept could be implemented through judicial interpretation of Article 28's purpose — to prevent superiors from avoiding liability due to inadequate oversight.[6,11,19-20,28] Legal scholars such as Alessandra Spadaro suggest reimagining command responsibility to include control over weapons, not only human troops.[19] Such a doctrine would close the loophole that allows commanders to evade responsibility by blaming technology.[3-5,19-21]

4.3. Creating New Offences and Prosecutorial Guidelines

Another solution is normative development — introducing new offences or guidelines specifically addressing AWS.[1-5,9,20] The international community could negotiate an amendment or protocol defining crimes like "launching an autonomous attack likely to cause indiscriminate harm".[1,3,5,9] This would make reckless or negligent use of AWS prosecutable, even without proof of specific intent to kill civilians.[1,3-5,11]

In the absence of formal amendments, the ICC Office of the Prosecutor could issue policy guidance on how to handle AWS-related cases. It could clarify evidentiary standards for establishing intent and causation, and encourage prosecutors to treat extreme recklessness in AWS deployment as a form of criminal negligence under Article 28 of the Rome Statute.[6,11,28] This evolution of prosecutorial practice could ensure accountability without breaching the principle of legality.[11,27-28]

4.4. Accountability Beyond Criminal Trials

Finally, accountability need not rely solely on criminal convictions. States remain responsible under international law for the unlawful use of their weapons.[3,11,28] State responsibility, reparations, and victim compensation schemes can provide redress where individual liability fails.[3,11,28] Truth commissions and public inquiries could also assign moral and political blame, even if criminal proof is lacking.[11,28]

Still, these are imperfect substitutes. As Human Rights Watch warns, the absence of personal accountability weakens deterrence and denies justice to victims.[1] The ultimate goal of international criminal law is to ensure that where grave suffering is caused, someone can be held to account.[11,28] Adapting the Rome Statute through interpretation, doctrine, and practice is therefore essential — not only to close the responsibility gap but to preserve the moral authority of international justice in the era of autonomous warfare.[1,3-6,11,19-20,28]

5. Conclusion

Autonomous weapon systems (AWS) present one of the most complex challenges to modern international criminal law. Under the current Rome Statute framework, holding individuals criminally liable for war crimes or crimes against humanity committed through AWS is possible but highly uncertain. Existing doctrines — such as indirect perpetration, aiding and abetting, and command responsibility — can, in theory, reach the human decision — makers who deploy or fail to control these systems. When an individual deliberately uses an AWS to commit atrocities, intent and control can be proven, and liability fits comfortably within existing law.

The real difficulty arises when AWS act unpredictably, causing unlawful harm that no human specifically intended. In such cases, strict application of traditional principles leaves a legal vacuum: no human actus reus, no intent, and no subordinate who can be punished. This "responsibility gap" threatens both justice for victims and the credibility of international criminal law.

To close this gap, the Rome Statute must be interpreted and applied in a way that reflects new technological

realities. Recognising a commander's duty to control their weapons — including autonomous systems — would ensure accountability when that duty is breached. Expanding command responsibility and acknowledging omission liability would align with the Statute's purpose: preventing impunity where human failure leads to serious crimes.

At the same time, the international community should continue to develop clearer legal norms—whether by clarifying intent standards for high-risk technologies or restricting fully autonomous lethal weapons altogether. Ultimately, victims of AWS — related atrocities deserve justice, and accountability must remain human. The ICC and its member states must ensure that as warfare evolves, so too does the law — so that no act of violence, however technologically advanced, escapes responsibility.

References

[1] Human Rights Watch, 2015, Harvard Law School International Human Rights Clinic. Mind the Gap: The Lack of Accountability for Killer Robots. New York: Human Rights Watch: 12–14.

[2] Docherty B L, 2012, Losing Humanity: The Case against Killer Robots[R]. New York: Human Rights Watch.

[3] Crootof R, 2016, War torts: accountability for autonomous weapons. University of Pennsylvania Law Review, 164(6): 1347–1402.

[4] Matthias A, 2004, The responsibility gap: ascribing responsibility for the actions of learning automata. Ethics and Information Technology, 6(3): 175–183.

[5] Chengeta T, 2016, Accountability gap: autonomous weapon systems and modes of responsibility in international law. Denver Journal of International Law and Policy, 45(1): 1–52.

[6] Rome Statute of the International Criminal Court, 1998, 2187 UNTS 90.

[7] Schmitt M N, 2015, Autonomous weapon systems and international humanitarian law: a reply to the critics. Harvard National Security Journal, 6: 1–36.

[8] Boothby W H, 2016, Weapons and the Law of Armed Conflict. 2nd ed. Oxford: Oxford University Press: 270–276.

[9] Asaro P, 2012, On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. International Review of the Red Cross, 94(886): 687–709.

[10] Sassòli M, 2019, International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare. Cheltenham: Edward Elgar: 417–420.

[11] Werle G, Jessberger F, 2020, Principles of International Criminal Law. 4th ed. Oxford: Oxford University Press: 178–186.

[12] Jain N, 2011, The control theory of perpetration in international criminal law. Chicago Journal of International Law, 12(1): 159–199.

[13] Ambos K, 2021, Article 25: individual criminal responsibility//Triffterer O, Ambos K (eds). The Rome Statute of the International Criminal Court: A Commentary. 4th ed. München; Oxford: Beck; Hart: 1250–1253.

[14] Block J, 2023, Responsibility for ordering under Article 25(3)(b) of the Rome Statute//Olásolo H (ed). Reconciling Responsibility with Reality: A Comparative Analysis of Modes of Active Leadership Liability in International Criminal Law. The Hague: TMC Asser Press: 367–411.

[15] Öztürk O, 2021, Does the purpose clause of Article 25(3)(c) of the Rome Statute cause impunity?. Australian International Law Journal, 28: 145–166.

[16] Werle G, 2007, Individual criminal responsibility in Article 25 ICC Statute. Journal of International Criminal Justice, 5(5): 951–969.

[17] Prosecutor V T, 1999, International Criminal Tribunal for the former Yugoslavia, Case No. IT-94-1-A, 185–226.

[18] Ambos K, 2007, Joint criminal enterprise and command responsibility. Journal of International Criminal Justice, 5(2): 159–183.

[19] Spadaro A, 2023, A weapon is no subordinate: autonomous weapons and the scope of superior responsibility. Journal of International Criminal Justice, 21(5): 1119–1144.

[20] Gaeta P, 2024, Who acts when autonomous weapons strike? The act requirement for individual criminal responsibility and state responsibility. Journal of International Criminal Justice, 21(5): 1033–1054.

[21] Devitt S K, 2023, Meaningful human command: advance control directives as a method to enable moral and legal responsibility for autonomous weapon systems. arXiv pre-print: 1–25.

[22] Duttwiler M, 2006, Liability for omission in international criminal law. International Criminal Law Review, 6(1): 35–57.

[23] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977, 1125 UNTS 3-06-08.

[24] Prosecutor v Delalić (Čelebići Case) (Trial Chamber Judgment). International Criminal Tribunal for the former Yugoslavia, 1998, Case No. IT-96-21-T, 333-346.

[25] Prosecutor V K, Ruzindana (Trial Chamber Judgment), 1999, International Criminal Tribunal for Rwanda, Case No. ICTR-95-1-T, 199-201.

[26] Caton J L, 2015, Autonomous Weapon Systems: A Brief Survey of Developmental, Operational, Legal, and Ethical Issues. Carlisle: Strategic Studies Institute, US Army War College: 23.

[27] Ambos K, 2013, Treatise on International Criminal Law, Vol. I: Foundations and General Part. Oxford: Oxford University Press: 297–299.

[28] Cryer R, Friman H, Robinson D, 2019, An Introduction to International Criminal Law and Procedure. 4th ed. Cambridge: Cambridge University Press: 3–5.