

Artificial Intelligence Crimes in Autonomous Weapon Systems and the Parties to Criminal and International Responsibility: An Analytical Study of State and Manufacturer Liability

Abolfath Khaleghi¹, Qays Riyadh Gatea²

¹ Professor of Criminal Law and Criminology, University of Qom, Qom, Islamic Republic of Iran

Email: ab-khaleghi@qom.ac.ir

² PhD Researcher in Criminal Law and Criminology, University of Qom, Qom, Islamic Republic of Iran

Email: qaisriyadh993@gmail.com

Abstract:

The rapid development of artificial intelligence technologies has significantly expanded their use in both civilian and military domains, particularly in robotics, autonomous weapon systems, and intelligent vehicles. This expansion has generated new forms of harmful and potentially criminal conduct that cannot be fully addressed through traditional rules of criminal and international responsibility. The central problem examined in this article concerns the identification of the party legally responsible for violations and damage caused by intelligent systems, given the multiplicity of actors involved in their design, programming, manufacture, operation, and deployment, together with the varying degrees of autonomy, learning capacity, and decision-making attributed to such systems. The article seeks to identify the principal offences that may be committed through artificial intelligence applications, analyse the legal risks associated with the use of autonomous weapon systems in armed conflict, and determine the scope of State responsibility for the conduct of its organs and armed forces. It further examines the responsibility of the State of registration or nationality and the liability of manufacturing companies for defects and damage caused by their products. Particular attention is given to the legal basis of State responsibility under the rules of attribution, due diligence obligations, and the duty to conduct legal reviews of weapons pursuant to Article 36 of Additional Protocol I of 1977.

The study employs descriptive and analytical methods by examining the characteristics of intelligent systems and analysing the relevant rules of criminal law, international humanitarian law, and the Articles on Responsibility of States for Internationally Wrongful Acts. It concludes that artificial intelligence, at its present stage of development, lacks the consciousness and legally recognised will required for independent criminal responsibility. Responsibility should therefore be attributed to the natural or legal persons, States, and entities that exercise authority over the design, operation, supervision, or deployment of such systems. States remain responsible for the conduct of their armed forces and for failures to test, review, and prevent unlawful outcomes, while manufacturers may incur liability for technical defects and unsafe products. The article recommends the adoption of a binding international framework governing autonomous weapon systems, the preservation of meaningful human control, and the establishment of effective mechanisms of accountability and reparation.

Keywords: artificial intelligence; autonomous weapon systems; criminal responsibility; State responsibility; manufacturers; international humanitarian law; due diligence.

1. Introduction

I. Background of the Study

Artificial intelligence has brought about a fundamental transformation in the nature of technologies used across different areas of life. Digital systems are no longer confined to executing pre-programmed commands; they are increasingly capable of processing vast quantities of data, learning from experience, adapting to changing conditions, and making decisions with varying degrees of independence from direct human intervention. This development has improved performance in industry, transport, medicine, security, and defence, but it has also generated complex legal and security risks.

The risks associated with artificial intelligence become particularly acute when the technology is incorporated into physical systems capable of causing direct harm, such as robots, self-driving vehicles,

unmanned aerial vehicles, and autonomous weapon systems. In such applications, programming errors, misuse, inadequate oversight, or external interference may cause serious bodily or material harm, including death, personal injury, destruction of infrastructure, or violations of international humanitarian law.

Autonomous weapon systems have become among the most controversial applications of artificial intelligence because of their potential capacity to detect, analyse, select, and engage targets without direct human intervention at every stage of the targeting cycle. Their use raises concerns about whether such systems can distinguish combatants from civilians, assess the proportionality of an anticipated military advantage against expected incidental harm, and take all feasible precautions during an attack.

The issue is not limited to the legality of using these systems; it also extends to the identification of the party responsible for the consequences arising from their operation. A single system may involve numerous actors, including programmers, designers, manufacturers, operators, military commanders, and the State that owns or deploys the weapon. In certain cases, it may be difficult to identify the person who performed the material act, possessed the requisite intent, or had the capacity to foresee and prevent the harmful result.

II. Research Problem

The research problem lies in the inability of traditional rules of criminal and international responsibility to provide a clear and comprehensive legal response to harmful acts resulting from the use of artificial intelligence, particularly autonomous weapon systems, in circumstances where these systems enjoy a degree of relative autonomy and where multiple actors participate in their design, production, and operation.

The problem becomes more complex when the system produces unexpected behaviour as a consequence of its ability to learn and adapt, or when it is impossible to determine whether the harm resulted from a defect in design, programming, training data, operation, maintenance, or the military decision to deploy the weapon. Such circumstances may create an accountability gap in which serious harm or a grave violation occurs without responsibility being attributable to a clearly identifiable person.

Further questions arise concerning State responsibility for conduct produced by autonomous weapon systems and the extent to which such conduct may be attributed to the State as an act of its armed forces or public organs. The liability of manufacturing companies for technical or software defects also requires examination, as does the adequacy of existing product-liability rules in addressing damage caused by intelligent military systems.

The principal research question is: To what extent are existing criminal and international legal rules adequate to identify the parties responsible for crimes and violations arising from the use of artificial intelligence and autonomous weapon systems, and what is the legal basis of State and manufacturer liability?

The principal question gives rise to the following subsidiary questions:

What are the principal crimes and risks resulting from artificial intelligence applications?

Can an artificial intelligence system itself be held criminally responsible?

What is the scope of responsibility borne by the programmer, operator, user, and military commander?

When may the conduct of an autonomous weapon system be attributed to a State?

What are the legal consequences of failing to satisfy due diligence obligations and the duty to conduct legal reviews of weapons?

To what extent are manufacturing companies liable for defects in intelligent systems and for the damage caused by them?

Can force majeure or the unforeseeability of a system's behaviour exempt a State from responsibility?

III. Significance of the Study

The academic significance of this article lies in its examination of a subject situated at the intersection of criminal law, international humanitarian law, the law of State responsibility, and the legal regulation of emerging technologies. The subject requires renewed consideration of several traditional concepts, including the criminal actor, will, fault, causation, effective control, and international attribution.

The article is also significant because it seeks to clarify the legal boundary between the use of artificial intelligence as a mere instrument of execution and situations in which an intelligent system possesses a high degree of autonomy that makes the identification of a responsible human actor more difficult. It further

contributes to explaining the relationship between individual criminal responsibility, the international responsibility of States, and the civil or criminal liability of manufacturing companies.

From a practical perspective, the subject is important because judicial, military, and regulatory bodies require workable standards for determining responsibility when harm occurs. Such standards are necessary to prevent technical complexity or the multiplicity of participating actors from becoming grounds for impunity. They are also essential for requiring States and companies to test, review, and monitor intelligent systems before deployment and to ensure their conformity with applicable legal and humanitarian rules.

IV. Objectives and Structure of the Study

This article seeks to define the concept of artificial intelligence crimes and identify their principal forms. It analyses the civilian and military applications of intelligent systems, with particular emphasis on robots and autonomous weapon systems.

It further aims to identify the parties that may incur criminal or international responsibility for damage resulting from such systems, explain State responsibility for the conduct of armed forces and public organs, and analyse the liability of manufacturing companies for technical and software defects.

The article also seeks to clarify the legal basis of State responsibility in light of the rules of attribution, due diligence, the duty to prevent harm, and the obligation to conduct legal reviews of weapons. It evaluates the adequacy of existing rules and proposes appropriate legislative and international solutions.

The article is divided into two principal sections. The first examines artificial intelligence crimes by addressing offences associated with robots and intelligent vehicles, the use of artificial intelligence in military applications, and the risks and advantages of autonomous weapon systems. The second examines the parties to criminal and international responsibility, including the responsibility of the State of nationality or registration, State responsibility for the conduct of its organs and armed forces, the liability of manufacturing companies, and the legal basis of State responsibility under the rules of attribution, due diligence, and the duty to conduct legal reviews of weapons.

Artificial Intelligence Crimes and the Parties to Criminal Responsibility

Against the backdrop of the rapid technological transformation witnessed worldwide, artificial intelligence has emerged as one of the most significant manifestations of contemporary digitalisation because of its extensive capacity to analyse data, make decisions, and perform tasks with a degree of efficiency that may exceed ordinary human capabilities. Notwithstanding its considerable advantages, this development has also generated new forms of unlawful conduct that pose serious threats to legal and social security.

Artificial intelligence has provided sophisticated means for committing novel offences and for enhancing traditional forms of criminality, including digital fraud, violations of privacy, manipulation of information, defamation, and the dissemination of false news. These developments have exposed the limitations of conventional criminal-law rules in addressing technologically mediated wrongdoing.

The danger of artificial intelligence-related crime is intensified by its technical complexity, the difficulty of detection, and the interdependence of human and machine roles in the commission of the relevant act. These characteristics raise difficult legal questions regarding the attribution of criminal responsibility.

The potential perpetrator is no longer confined to a single natural person. Responsibility may involve programmers, operators, users, owners, and entities benefiting from the artificial intelligence system. This multiplicity of actors raises fundamental questions concerning the legal basis and limits of criminal responsibility and the possibility of attributing the offence to a particular person where an intelligent system participates in its execution.

Accordingly, the examination of artificial intelligence crimes and the parties to criminal responsibility is necessary to assess whether existing criminal legislation can accommodate these emerging offences and whether legal rules must be developed to ensure criminal justice while keeping pace with technological change.

This part is divided into two sections. The first addresses artificial intelligence crimes, while the second examines the parties who may incur criminal responsibility in the field of artificial intelligence.

Section One: Artificial Intelligence Crimes

The rapid development of artificial intelligence technologies has produced forms of criminal conduct that were previously unknown, thereby creating serious challenges for traditional criminal-justice systems. Artificial intelligence may be used to commit offences affecting individuals and society, including data

manipulation, invasions of privacy, and electronic fraud.

Artificial intelligence crimes are characterised by technical complexity and difficulties of detection, which in turn generate problems of criminalisation and proof. This reality requires the reconsideration of criminal legislation to ensure that it keeps pace with technological progress and provides effective protection for legally protected interests.

This section is divided into two subsections. The first examines offences associated with artificial intelligence-enabled machines and systems, while the second addresses the use of artificial intelligence in military applications.

Subsection One: Offences Associated with Artificial Intelligence Systems

Many machines employing artificial intelligence technologies are already present in contemporary life, including robots, aircraft, vessels, and vehicles. Intelligent vehicles are among the applications most closely connected to everyday human activity because they are more widely available than many other intelligent machines. The discussion below therefore addresses offences involving robots and autonomous vehicles and examines well-known incidents associated with their operation.

I. Offences Involving Robots

Following the end of the nineteenth century and the development of modern machinery capable of performing sustained work for longer periods than human labourers, advances in navigation assistance and manufacturing mechanisms created the first genuine opportunity to move towards machine automation and reduce direct human participation in production processes. The modern robot emerged from this combination of technical innovation and social transformation.¹

Robotics constitutes one of the principal branches of artificial intelligence. It integrates electrical engineering, mechanical engineering, and computer science for the design, construction, and operation of robots. Alan Turing famously anticipated that computers would become capable of sophisticated forms of imitation by the beginning of the twenty-first century.²

Robotic movement varies according to design. Certain robots use articulated arms capable of rotating in several directions, whereas others are restricted to linear movement. Concepts such as degrees of freedom and degrees of movement are therefore important when assessing a robot's physical configuration and the operational space within which it functions.³

Armed forces are traditionally divided according to their operational environments into land, naval, air, and defensive or offensive missile forces. The development of autonomous intelligent weapons has led to their incorporation into each of these military domains alongside civilian applications. Such systems may be prepared to perform combat functions more effectively while reducing risks to human personnel. Initially, autonomous systems were used in armed conflict primarily for surveillance. Their offensive use was avoided because of anticipated adverse consequences. Subsequent practice, however, has demonstrated that the acquisition of technology capable of providing a decisive advantage over an adversary frequently leads to the abandonment of the system's original limited purpose.⁴

Technological advances have enabled robots to participate in field testing, including underwater operations. Some systems can descend to significant depths, remain operational for several hours, and move at high speed. Such capabilities reveal their potential military utility and explain why many commentators expected underwater autonomous systems to emerge before comparable land-based applications, partly because their use was perceived as presenting a lower risk of civilian casualties.⁵

Outer space is also regarded as an important field for the deployment of autonomous intelligent systems. As outer space may become an arena of military operations during the twenty-first century, the weaponisation of space has increasingly appeared among the priorities of future military strategy. Nevertheless, the use of autonomous weapons in outer space raises issues that differ from those normally

¹Haitham Issa, *The Pre-Contractual Duty to Explain through Artificial Intelligence Systems* (Dar Al-Nahda Al-Arabiya, Cairo, 2018), p. 32 [Arabic].

²Ahmed Al-Sherbini and Wafaa Baghdadi, *Internet Protection and Security: The Coming Challenge and Methods of Response* (Egyptian General Book Authority, Cairo, 2010), p. 154 [Arabic].

³Blay Whitby, *Artificial Intelligence*, trans. Translation Department of Dar Al-Farouq (Dar Al-Farouq for Cultural Investments, Egypt, 2008), p. 159 [Arabic translation].

⁴Anwar Mahmoud Abdel-Wahed and Ahmed Amin Abdel-Majid, *The Robot between Imagination and Science* (Al-Ahram Centre for Translation and Publishing, Cairo, 2002), p. 41 [Arabic].

⁵T. X. Hammes, "War Robots: How Artificial Intelligence Will Change the Nature of Future Wars," Future Center for Advanced Research and Studies, 4 July 2017, available at Future UAE, accessed 22 November 2025 [Arabic source].

encountered in conventional armed conflicts.⁶

II. Offences Involving Intelligent Autonomous Vehicles

Self-driving vehicles are among the best-known automated applications of artificial intelligence. Numerous companies have conducted experimental operations of autonomous vehicles with a view to broader commercial deployment. An examination of their operating mechanisms is necessary in order to determine who may incur criminal responsibility for offences or harmful incidents arising from their use and how the causal relationship between a responsible actor and the resulting harm may be established.⁷

An autonomous vehicle operates through artificial intelligence software that issues commands concerning movement, direction, and stopping after receiving data from radar, laser, camera, and sensor systems. These devices collect information concerning pedestrians, road dimensions, surrounding vehicles, and other objects in the immediate environment. The artificial intelligence programme analyses these data and issues operational commands. Its operating architecture may resemble the systems used in mobile phones or computers and is commonly connected to cloud-based data storage.

The stored data function in a manner comparable to an aircraft's flight recorder. They may preserve information relating to the vehicle's movements, commands, and decisions, thereby enabling investigators to reconstruct an incident and identify its technical or human cause.

One of the most widely reported fatal incidents involving an autonomous vehicle occurred in March 2018, when a self-driving vehicle operated by Uber struck a pedestrian who subsequently died from her injuries. Although the incident attracted substantial public attention, many commentators supported the continuation of autonomous-vehicle testing on the ground that human drivers cause comparable or more serious accidents and that autonomous vehicles may ultimately prove safer than human-operated vehicles.⁸

III. Self-Defence and Artificial Intelligence Systems

A further question, although it may initially appear hypothetical, concerns whether an artificial intelligence system may benefit from grounds of justification or exclusions of responsibility comparable to those recognised for natural persons.

Suppose that the direction of harm is reversed and a human being deliberately strikes a robot with a vehicle or attacks and attempts to destroy it using another instrument. Could the robot exercise a right of self-defence? Would the human attacker incur criminal responsibility, or would the matter be confined to civil liability and compensation?

Under existing Iraqi and Egyptian criminal legislation, the right of self-defence is framed primarily around the protection of human life and property and does not confer an independent personal right of self-defence upon a robot, regardless of its technical capabilities. Article 42 of the Iraqi Penal Code No. 111 of 1969, as amended, provides that an act does not constitute an offence when committed in the lawful exercise of self-defence, provided that an imminent danger of an offence threatens the defender or another person, or their property; recourse to the public authorities is not reasonably possible in time; and no other means is available to avert the danger.¹⁰

Most Arab criminal legislation remains far removed from the rapid development of artificial intelligence technologies and generally contains no comprehensive regulation defining the rights and obligations associated with artificial intelligence entities.¹²

A distinction must nevertheless be drawn between a robot defending itself and a robot protecting a human being. Although the statutory rules governing defence of oneself or another were drafted with human actors in mind, it would be unreasonable to prevent an artificial intelligence system from intervening to protect a human being or that person's property, provided that the system can distinguish an unlawful attack

⁶Abu Bakr Muhammad Al-Deeb, *Military Applications of Artificial Intelligence in Light of Public International Law* (Dar Al-Nahda Al-Arabiya, Egypt, 2021), p. 66 [Arabic].

⁷Patrick Hubbard, "Sophisticated Robots: Balancing Liability, Regulation, and Innovation," *Florida Law Review* (2014), p. 1803.

⁸These views appeared in responses to Uber's official Twitter announcement concerning the suspension of autonomous-vehicle testing, accessed 22 November 2025.

⁹Aarian Marshall and Alex Davies, "Uber's Self-Driving Car Saw the Woman It Killed," *Wired*, available online, accessed 22 November 2025.

¹⁰Article 42 of Iraqi Penal Code No. 111 of 1969, as amended and in force.

¹¹Najati Sayyid Ahmad Sanad, *Principles of the General Part of Criminal Law: Crime and Punishment* (Faculty of Law, Zagazig University, 2011), p. 479 [Arabic].

¹²Abdel-Tawab Moawad Al-Shuraihi, *Lessons in Criminal Law: General Part* (Faculty of Law, Zagazig University, 2017), p. 246 [Arabic].

and assess the requirement of proportionality between the attack and the defensive response.¹³

A related question is whether an individual may programme a robot to defend them when attacked. Such programming may be legally defensible only where the robot possesses sufficient technical capacity to assess the nature of the attack and maintain proportionality in its response. Where the system lacks that capacity, the owner or programmer should not be permitted to deploy it as an unrestricted defensive mechanism. If disproportionate force is used, the responsible human actor may incur criminal liability because the robot functions as an instrument through which the offence is committed, and the requirements of lawful self-defence are not satisfied.¹⁴

As to a robot's defence of its own physical integrity, current law does not recognise an independent right of self-defence belonging to the machine. Some commentators nevertheless argue that future legislation may need to distinguish between highly advanced systems capable of controlled, proportionate responses and less sophisticated systems incapable of reliable discrimination. An advanced robot capable of evaluating the attack and calibrating its response might arguably be authorised to protect itself, whereas an uncontrolled system should not be permitted to use force because the protection of human life remains superior to the preservation of replaceable machinery.¹⁵

Any future recognition of such a limited defensive capacity would therefore have to be restricted to advanced systems demonstrably capable of distinguishing an attack, evaluating necessity, and maintaining proportionality. The manufacturer's technical documentation and system-design records would be central to determining whether those requirements were satisfied.

Subsection Two: The Use of Artificial Intelligence in Military Applications

The risks posed by lethal autonomous weapon systems have attracted increasing international concern since the global Campaign to Stop Killer Robots was launched in London on 23 April 2013. An assessment of the advantages and disadvantages associated with the use of robotic systems in combat is essential to any analysis of their legal implications. This subsection therefore examines the principal risks and benefits identified in academic literature and in discussions conducted under the auspices of the United Nations.¹⁶

I. The Use of Intelligent Weapons in Combat and the Resulting Risks

Methods used to destroy or corrupt data and software range from computer viruses and worms to logic bombs and time bombs. Information-related criminality constitutes one of the principal forms of unlawful interference with digital technology and may create exceptionally serious consequences when directed against military systems.¹⁷

The increasing use of automated information-processing techniques has not produced exclusively beneficial effects. In practice, such systems may be exploited abusively or used in bad faith. Information systems may also be deliberately destroyed or disabled, not merely to obtain an unlawful benefit, but to damage the system itself and prevent it from performing its intended functions.¹⁸

One of the most serious criticisms directed at artificial intelligence is that a machine lacks consciousness and may be unable to distinguish lawful commands from unlawful ones. During the 2015 Meeting of the High Contracting Parties to the Convention on Certain Conventional Weapons, several delegations expressed concern about the unpredictability of machine behaviour, particularly where systems are deployed in unfamiliar or complex environments.

The non-deterministic character and technical complexity of advanced systems may render comprehensive testing extremely difficult, if not impossible. Possible safeguards discussed in this context include restricting the operation of lethal autonomous weapon systems by time and geographical area and equipping them with self-deactivation or self-destruction mechanisms that operate if the system is captured, compromised, or suffers a critical malfunction.

¹³Najati Sayyid Ahmad Sanad, *Principles of the General Part of Criminal Law*, above n 10, p. 515.

¹⁴Abdel-Tawab Moawad Al-Shuraihi, *Lessons in Criminal Law: General Part*, above n 12, p. 27.

¹⁵Compare Article 56(4) of Federal Penal Code No. 3 of 1987 of the United Arab Emirates regarding natural persons; by analogy, a similar rationale may be considered in relation to advanced robotic systems.

¹⁶The Campaign to Stop Killer Robots was launched in London on 23 April 2013. The original Arabic manuscript also refers to public discussion surrounding an incident in Las Vegas in 2019 involving a Tesla vehicle and a robot.

¹⁷Abu Bakr Muhammad Al-Deeb, *Military Applications of Artificial Intelligence in Light of Public International Law* (Dar Al-Nahda Al-Arabiya, Egypt, 2021), p. 488.

¹⁸Muhammad Sami Al-Shawwa, *The Information Revolution and Its Implications for Criminal Law* (Dar Al-Nahda Al-Arabiya, Cairo, 2003), p. 4.

Robotic systems are frequently expensive to develop and maintain. Their effective deployment requires substantial expenditure on programming, maintenance, engineering, testing, and technical infrastructure. Successful artificial intelligence programmes therefore commonly depend on large-scale and resource-intensive projects.

A further problem concerns the ability of robots to respond to dispersed, unfamiliar, and unpredictable situations. Although relevant knowledge about the real world may be incorporated into a system, certain functions still require human assistance, particularly tasks involving contextual judgment, qualitative reasoning, or the selection of solutions in novel circumstances.¹⁹

Robots may be highly effective in processing quantitative problems, but their ability to perform qualitative assessments remains limited. Such assessments are often indispensable where human life is at stake and where the legal and ethical implications of a decision cannot be reduced to numerical calculation.

The possibility of espionage constitutes another major risk. The widespread use of computers has concentrated sensitive information within increasingly interconnected systems, thereby facilitating access to industrial, commercial, professional, and military secrets. Digital systems have consequently been compared to safes without doors.²⁰

Communications between the human actor exercising control and the machine may be interrupted, intercepted, or manipulated by an adversary. A lethal autonomous weapon system may also malfunction because of defective coding or may be compromised by a cyberattack conducted by a hostile State or a non-State actor.

The 2015 discussions concerning the Convention on Certain Conventional Weapons examined emerging approaches for managing the potential risks associated with lethal autonomous weapon systems. Participants considered scenarios in which the risks arose from the technology itself and recognised that systems capable of autonomous operation in complex environments were likely to possess a high degree of technical sophistication.

Such complexity may not be fully understood by those who operate or deploy the system. It can therefore generate risks that the human operator cannot reasonably anticipate. These risks may be aggravated when different systems or software components are combined and when automated interactions occur at a speed that exceeds meaningful human supervision.

The speed of machine interaction, together with the complexity of software and the capacity of certain systems to learn from experience, may weaken the ability of commanders and operators to predict the actions of autonomous weapons. The Fifth Review Conference concerning autonomous weapon systems in 2016 similarly highlighted the difficulty of predicting machine conduct in complex environments without some form of human supervision. It also identified a potential risk of escalation where more than one party to an armed conflict deploys such systems.

At the same time, computers and automated information processing provide important services to scientific and medical research and enable institutions and public administrations to organise their work more effectively. Nevertheless, the widespread use of computers and the Internet has also contributed to a substantial increase in information-related crime.²¹

II. The Use of Intelligent Weapons in Combat and the Resulting Advantages

The success and widespread use of modern robots may be attributed to two principal factors: ease of programming and the capacity to perform tasks by using sensory information received from the operational environment. Automated information processing has become indispensable across virtually every sector of human activity.²² Robots also possess an exceptional capacity to store information.²³

Robotic systems can receive and process a greater quantity of information simultaneously and at a higher speed than human beings. They may also operate in diverse and hazardous environmental conditions in which the deployment of human personnel would be dangerous or impracticable.

19 Blay Whitby, *Artificial Intelligence*, trans. Translation Department of Dar Al-Farouq (Dar Al-Farouq for Cultural Investments, Egypt, 2008), p. 166.

20 Marco Sassòli, "Autonomous Weapons and International Humanitarian Law: Advantages, Technical Questions, and Legal Issues Requiring Clarification," *International Committee of the Red Cross publication* (Cairo, 2017), p. 160.

21 Osama bin Ghanem Al-Obaidi, "International Efforts to Combat Information Crime," *Journal of Law*, no. 39 (Kuwait, 2015), p. 140.

22 Muhammad Sami Al-Shawwa, *The Information Revolution and Its Implications for Criminal Law*, above n 18, p. 3.

23 Edwin Wise, *Robot Manufacturing Technology* (Dar Al-Farouq for Cultural Investments, Egypt, 2009), p. 9.

Robots can provide consistent levels of performance because they are not affected by fatigue, boredom, fear, or emotional pressure. Advances in computing may also enable them to make rapid decisions and engage targets with high levels of technical precision. An autonomous aircraft assigned to attack a specified target may, for example, achieve greater accuracy and react more rapidly than a remotely piloted aircraft.

Military planners throughout the world have recognised the operational advantages of unmanned and autonomous combat vehicles. They may be less expensive to manufacture and operate than aircraft requiring human pilots and may reduce the personnel and infrastructure needed for certain missions. Nevertheless, modern unmanned aircraft still commonly require pilots, sensor operators, technicians, intelligence analysts, and other support personnel.

One of the most important advantages of autonomous systems is their ability to remain operational for long periods without fatigue. Human soldiers are vulnerable to illness, exhaustion, distraction, and boredom, whereas robots do not require leave or ordinary rest periods and generally cease operation only for maintenance, recharging, repair, or technical adjustment.

The use of robots may also protect military personnel from the physical and psychological consequences of combat, including death, serious injury, permanent disability, and trauma-related disorders. This protective function is frequently presented as one of the strongest practical arguments in favour of military robotics.²⁴

Military robots may also avoid certain emotional and psychological factors that contribute to violations committed by human combatants. Soldiers who have experienced violence, loss, fear, or trauma may themselves become more likely to commit violations of international humanitarian law. Machines do not experience revenge, hatred, panic, hunger, or an instinct for self-preservation.

This observation does not mean that robots are inherently humane. Human beings are responsible for designing, programming, authorising, and deploying the system. Nevertheless, some experts argue that a carefully designed autonomous system may comply more consistently with predefined legal constraints than a human soldier operating under extreme battlefield pressure.

Robots do not forget information, experience physical fear, or become exhausted. Certain United Nations discussions have therefore acknowledged that robotic systems might serve humanitarian purposes in some contexts, particularly where their flexibility and programmability enable adaptation to changing operational circumstances.²⁵

From this perspective, the person who designs and constructs an autonomous weapon in a controlled peacetime environment may be capable of embedding international humanitarian law constraints more systematically than a soldier can apply them in a hostile and rapidly changing battlefield. Such an argument remains controversial, but it demonstrates why the legal assessment of autonomous weapons must distinguish between different levels of autonomy, design, predictability, and human control.

The contemporary structure of asymmetric armed conflict also affects this assessment. Where one party possesses overwhelming technological superiority, the weaker party may have powerful incentives to disregard international humanitarian law. Non-compliance may consequently become a recurring structural feature of the conflict rather than an isolated incident confined to a particular time or place.²⁶

The risks associated with autonomous weapons are generally different in scale from those posed by nuclear weapons, which threaten cities, continents, humanity, and the global environment. Many risks associated with autonomous systems may remain more technically manageable where the weapons are limited in destructive capacity, geographic range, and operational autonomy.

A general rejection of automated information-processing technology would therefore disregard its substantial civilian and military benefits. A different conclusion may, however, be required for fully autonomous lethal systems whose effects are indiscriminate, whose conduct cannot be reliably predicted, and whose targets or consequences cannot be effectively controlled. Systems possessing these characteristics

²⁴ Edwin Wise, *Robot Manufacturing Technology*, above n 23, p. 349.

²⁵ Muhammad Salah and Ahmed Ahedy, *The Artificial Robot* (Dar Al-Kutub Al-Ilmiyya for Publishing and Distribution, Egypt, 2009), p. 12.

²⁶ Robin Geiss, "Asymmetric Conflict Structures," selections from the *International Review of the Red Cross*, vol. 88, no. 864 (Cairo, 2006), p. 237. See also Mahmoud Hijazi Mahmoud Basal, "State Management of Legal Risks Associated with Space Activities," Conference on Law and Technology, Faculty of Law, Ain Shams University (Egypt, 2017), p. 1603; and Hisham Omar Ahmad Al-Shafi'i, *International Responsibility for Damage Arising from Nuclear Space Activities* (Al-Dalil Company for Studies, Training, Printing and Publishing, Egypt, 2013), p. 13.

may create risks sufficiently grave to justify a comprehensive prohibition.

Section Two: Parties to Criminal and International Responsibility in the Field of Artificial Intelligence

The use of artificial intelligence has generated complex legal questions concerning the identification of the persons and entities that may incur criminal responsibility for unlawful conduct produced through intelligent systems. The criminal act may no longer be connected to a single individual. Instead, the roles of the programmer, operator, user, system owner, military commander, State authority, and manufacturer may overlap.

This multiplicity of actors makes it difficult to identify the person who possesses the requisite mental element and to distinguish the principal offender from an accomplice or merely negligent participant. These difficulties expose the limitations of traditional criminal-law doctrines when they are applied to systems whose conduct may be partially autonomous, adaptive, or technically opaque.

A coherent legal framework must therefore clarify the responsibility of the State of nationality or registration, the responsibility of States for the conduct of their organs and armed forces, and the liability of manufacturers whose products contain technical or software defects. This section is divided into two subsections. The first examines State and manufacturer responsibility, while the second addresses the legal basis of State responsibility for artificial intelligence systems.

Subsection One: Responsibility of the State of Nationality, State Organs, and Manufacturing Companies

I. Responsibility of the State of Nationality or Registration

An intelligent weapon may be described as an automated, mobile, or manually deployable machine designed to perform multiple functions and capable of executing movements without continuous human direction.²⁷ By analogy with ships and aircraft, some commentators argue that such a system may be connected to a State through registration, nationality, ownership, or deployment, notwithstanding the obvious differences between an autonomous weapon and conventional registered vehicles.²⁸

Human-rights organisations participating in the international Campaign to Stop Killer Robots have consequently advocated a comprehensive prohibition on the development, manufacture, use, and transfer of fully autonomous lethal weapons.²⁹ Their central concern is that the absence of meaningful human control may result in civilian casualties and violations of international humanitarian law while simultaneously making individual criminal accountability exceptionally difficult.

Article 23(e) of the 1907 Hague Regulations prohibits weapons, projectiles, or material calculated to cause unnecessary suffering. Article 35(2) of Additional Protocol I of 1977 reaffirms the principle by prohibiting weapons, projectiles, material, and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.³⁰

Although these provisions do not expressly refer to autonomous weapon systems, they apply to new technologies insofar as the weapon, by its nature or expected effects, causes unnecessary suffering or produces indiscriminate consequences. If an autonomous weapon cannot reliably distinguish lawful military objectives from civilians or persons hors de combat, the State that uses or deploys it may incur international responsibility for violating applicable treaty and customary rules.

Accordingly, where an autonomous weapon is attributed to a State through registration, ownership, control, or deployment, the State of nationality or registration may be required to answer for the internationally wrongful consequences of its use. The absence of a treaty devoted specifically to autonomous weapon systems does not remove the applicability of general international humanitarian law.

II. State Responsibility for the Conduct of Its Organs and Armed Forces

Under international law, the conduct of any State organ is regarded as an act of that State. The term “State organ” includes any person or entity possessing that status under the internal law of the State.³¹

27 Safat Amin Salama, *Weapons of Future Wars between Imagination and Reality* (Emirates Center for Strategic Studies and Research, United Arab Emirates, 2019), p. 12.

28 Duaa Jalil Hatem, “Autonomous Weapons and International Responsibility,” *Journal of Legal Sciences*, special issue (Iraq, 2020), p. 114.

29 Hamza Harqous, “A War without a Soul: Before the Robot Kills You,” *Al-Akhbar Magazine* (Lebanon, 2018), p. 1.

30 Article 35(2), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), 1977.

31 Ali Muhammad Kazim Al-Mousawi, *Direct Participation in Cyber Attacks* (Modern Book Institution, Beirut, 2019), p. 167.

Conduct may also be attributed to the State where a person or entity, although not formally an organ, is empowered by domestic law to exercise elements of governmental authority and acts in that capacity in the particular instance.³²

A State that deploys an autonomous weapon is the appropriate subject to bear international responsibility for the conduct generated through that weapon. Article 4 of the Articles on Responsibility of States for Internationally Wrongful Acts provides that the conduct of any State organ shall be considered an act of that State under international law. The machine itself is not an organ in the legal sense; however, the decision to design, approve, deploy, and operate the system is undertaken through human organs, military units, and public authorities.

The autonomous weapon should therefore be treated as an instrument through which the State organ acts. Where military personnel deploy the system in the course of official functions, the resulting operation is attributable to the State even if the system selects or engages a target through automated processes. Technical autonomy does not sever the legal connection between the weapon and the State authority that placed it into operation.

Attribution also follows from Article 91 of Additional Protocol I, which provides that a party to the conflict is responsible for all acts committed by persons forming part of its armed forces and must pay compensation where required.³³ This rule reflects the general principle that a State committing an internationally wrongful act must make full reparation for the injury caused.³⁴

The International Criminal Tribunal for the former Yugoslavia confirmed in the *Furundžija* judgment of 1998 and the *Tadić* Appeals Judgment of 1999 that States bear responsibility for the conduct of their armed forces.³⁵ Customary international humanitarian law likewise recognises State responsibility for violations attributable to State organs, including the armed forces.

Consequently, where a member of the armed forces deploys an autonomous weapon as part of an official military operation, the conduct resulting from the weapon is attributable to the State. The State may be required to cease the violation, provide assurances of non-repetition, investigate the incident, prosecute responsible individuals where appropriate, and make full reparation for the damage caused.

The compensatory dimension of State responsibility is well established in international practice. Following Iraq's invasion of Kuwait in 1990 and the subsequent Gulf conflict, the United Nations Security Council established mechanisms for compensating losses resulting from the internationally wrongful conduct.³⁶ Although the factual and legal context differs, the example demonstrates that State responsibility may entail organised and extensive reparations.

Applied to autonomous weapons, an indiscriminate attack conducted by a system deployed by State armed forces may therefore engage the responsibility of that State. The State cannot avoid responsibility merely by arguing that the software generated an unexpected targeting decision. The relevant legal act includes the human and institutional decisions to acquire, test, authorise, programme, maintain, and deploy the weapon.

III. Liability of Manufacturing Companies

The technological expansion that began during the twentieth century transformed both the variety and quantity of manufactured products. Modern markets now contain consumer goods, household devices, computers, vehicles, complex industrial systems, and numerous categories of weapons manufactured in extremely large quantities.

Holding a manufacturer liable for the failure of its product is a logical extension of product-liability principles. A company may be responsible for damage caused by defects in design, manufacture, programming, warnings, testing, cybersecurity, or maintenance instructions.³⁷ In principle, an action against

32 Muhammad Mahmoud Amin, *The Theory of the Internationally Wrongful Act: A Study of International Responsibility*, PhD thesis, College of Law, University of Baghdad (2007), p. 33.

33 Article 91 of Additional Protocol I of 1977 provides that a party to the conflict that violates the Geneva Conventions or the Protocol shall, where appropriate, be liable to pay compensation and shall be responsible for all acts committed by persons forming part of its armed forces.

34 Ahmed Abu Al-Wafa, *International Law and International Relations* (Dar Al-Nahda Al-Arabiya for Publishing and Distribution, Cairo, 2005), p. 504.

35 Najat Ahmad Ahmad Ibrahim, *International Responsibility for Violations of International Humanitarian Law* (Munsha'at Al-Ma'arif, Alexandria, 2009), p. 292.

36 Ahmed Abu Al-Wafa, *International Law and International Relations*, above n 34, p. 505.

37 Patrick Lin and Keith Abney, "Autonomous Military Robotics: Risk, Ethics, and Design," California Polytechnic State

the manufacturer may be based on product liability, negligence, contractual responsibility, or, in particularly dangerous activities, strict liability.

Product-liability claims nevertheless present jurisdictional difficulties, particularly where the manufacturer is located abroad or where components, software, and training data originate in several jurisdictions. National courts must determine whether they possess jurisdiction over the manufacturer and which law applies to the claim.

The law governing liability for defective products has undergone significant development through international organisations, legislation, judicial decisions, and legal scholarship.³⁸ Many legal systems have strengthened the protection afforded to consumers and injured persons by recognising a distinct regime of producer liability. French civil law incorporated a specialised defective-product regime in 1998, while a number of Arab legal systems adopted comparable rules later, including Algeria in 2005.³⁹

The concept of “producer” is interpreted broadly in many legal systems. It may include the actual manufacturer of the finished product, the producer of raw materials, the manufacturer of component parts, and a person who places a name, trademark, or other identifying mark on the product and presents it to the market as their own.⁴⁰

International efforts have also addressed the applicable law in product-liability disputes. The Hague Conference on Private International Law considered the subject during the 1960s and ultimately adopted the 1973 Hague Convention on the Law Applicable to Products Liability.⁴¹ The Convention reflects the international character of modern production and the need to identify the law governing claims involving manufacturers, injured persons, and products connected to different States.

A person injured by a defective product may include any individual who suffers physical or material damage as a result of using or being exposed to the product, even where no contractual relationship exists between the injured person and the manufacturer.⁴² This approach reduces the traditional distinction between contractual and tortious liability and expands protection to all persons harmed by the defective product.

In the context of autonomous weapons, reliance exclusively on ordinary civil liability may remain inadequate because national law may narrowly define the circumstances in which a manufacturer is liable for the failure of a military product. This limitation may be addressed through strict liability for ultrahazardous activities and dangerous products, particularly where the harm results from an inherent risk associated with unpredictable automated conduct.

A company that sells or supplies an autonomous weapon may therefore incur liability for bodily or material damage caused by the system. Where the risk materialises because of a design defect, defective software, inadequate testing, insufficient safeguards, or a failure to warn the purchasing State of foreseeable limitations, liability should not depend entirely on proving subjective fault.

The assessment must nevertheless distinguish between a product defect and an unlawful operational decision made by military authorities. Manufacturers should not automatically bear responsibility for every unlawful use of a technically compliant weapon. Conversely, States should not be permitted to shift responsibility to manufacturers where the State knowingly deployed a system outside its approved operational parameters or failed to conduct the required legal and technical review.

Subsection Two: The Legal Basis of State Responsibility for Artificial Intelligence

Where unlawful conduct cannot be attributed directly to a State, the State is not automatically responsible for the conduct itself. It may nevertheless remain bound by a duty of due diligence to control foreseeable risks before harm occurs. States must therefore take appropriate measures to ensure that the use of autonomous weapon systems complies with international humanitarian law. This obligation requires the prevention and mitigation of risks during the development, testing, acquisition, and deployment of such

University, San Luis Obispo (2008), pp. 55–56.

38 Salim Muhammad Radī'an Al-Azzawi, *Producer Liability in Civil Laws and International Conventions*, 2nd edn (Dar Al-Thaqafa for Publishing and Distribution, Amman, 2009), p. 31.

39 Muammar Bin Taria, “The Concept of Product Defectiveness in the Producer’s Civil-Liability Regime and Insurance Solutions: A Comparative Study,” *Kuwait International Law School Journal*, year 6, no. 22 (2018), p. 647.

40 Hussein Farhi, *Civil Liability of the Producer*, Master’s thesis, Faculty of Law and Political Science, Larbi Ben M’hidi University, Oum El Bouaghi, Algeria (2014), p. 27.

41 Duaa Jalil Hatem, “Autonomous Weapons and International Responsibility,” above n 28, p. 121.

42 Saaoui Celia, *Civil Liability of the Producer for Damage Caused by Defective Products*, Master’s thesis, Faculty of Law and Political Science, Abderrahmane Mira University, Algeria (2017).

weapons.

The legal basis for this obligation may be derived from Common Article 1 of the four Geneva Conventions of 1949, under which the High Contracting Parties undertake to respect and ensure respect for the Conventions in all circumstances. This formulation requires States not only to refrain from violating the law of armed conflict, but also to adopt appropriate measures to prevent violations within the limits of their authority and capacity.⁴³

Due diligence is an obligation of conduct rather than an absolute guarantee of a particular result. It requires a State to employ the best efforts reasonably available to prevent internationally wrongful conduct. International jurisprudence concerning the duty to prevent genocide illustrates that a State must use all means reasonably available to it, even though the obligation does not guarantee that prevention will always succeed.

The required degree of diligence increases in proportion to the seriousness and foreseeability of the risk. The deployment of an autonomous system within a geographically restricted and sparsely populated operational environment may require a different level of precaution from deployment in a complex urban area populated by civilians. The greater the potential harm and uncertainty, the more rigorous the obligations of testing, supervision, and control.⁴⁴

This duty is reinforced by Article 36 of Additional Protocol I of 1977, which requires each State Party, in the study, development, acquisition, or adoption of a new weapon, means, or method of warfare, to determine whether its employment would, in some or all circumstances, be prohibited by international law.

A legal review under Article 36 must consider the ordinary and reasonably foreseeable uses of the weapon. It should determine whether a particular autonomous system has been designed, manufactured, trained, or programmed in a manner capable of producing effects prohibited by international humanitarian law. Such a review must examine, among other matters, the system's capacity to distinguish lawful targets, assess expected incidental harm, remain within spatial and temporal limits, respond to changes in the operational environment, and permit meaningful human intervention.

The review cannot be treated as a one-time administrative formality. Autonomous systems may change through software updates, machine-learning processes, new training data, or integration with other platforms. A substantial technical modification may therefore require a renewed legal and operational review. In the absence of careful testing and review, responsibility for foreseeable unlawful effects may be attributed to the State that authorised development or deployment.

The assessment of responsibility must also distinguish between rules requiring only an objectively unlawful result and rules that require a specific mental element, such as intent, recklessness, or negligence. Autonomous systems do not possess legally recognised intent. Where the violated rule requires a culpable mental state, responsibility must therefore be examined through the conduct of the human actors who designed, authorised, deployed, supervised, or failed to control the system.⁴⁵

Where the applicable rule is breached by the objective consequences of an attack, the absence of machine intent does not eliminate State responsibility. The conduct may still be attributed to the State through the persons and organs that selected and deployed the weapon, particularly where they exercised effective control over the operation. The International Court of Justice applied the effective-control standard in the *Military and Paramilitary Activities in and against Nicaragua* case when assessing the relationship between the United States and the Contra forces.

If a violation requires proof of fault, the person who authorised or deployed the weapon becomes central to the legal analysis. That person may incur responsibility where the system was used despite known limitations, inadequate testing, foreseeable risks, or an inability to comply reliably with the applicable rules.

The technical complexity of autonomous weapon systems is one of the principal obstacles to attribution. Commanders and operators may not understand every element of the software or learning architecture, especially after deployment. Nevertheless, legal responsibility cannot be avoided merely because the system is technically complex. An operator need not understand every line of code, but must understand the system's operational capabilities, limitations, foreseeable behaviour, and suitability for the

43 Du'a Jalil Hatim, "Autonomous Weapons and International Responsibility," above, p. 121.

44 Du'a Jalil Hatim, "Autonomous Weapons and International Responsibility," above, p. 118.

45 International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts and Commentaries* (2001), pp. 43–59.

assigned mission.⁴⁶⁴⁷

If the system's characteristics prevent meaningful control during a material phase of deployment, the appropriate legal response is not to disregard responsibility but to refrain from deployment. A State may therefore incur responsibility for damage caused by an autonomous system where it authorised the use of a weapon whose behaviour could not be predicted or controlled with the degree of reliability required by the operational environment.

Predictability may decrease as the duration of operation and environmental complexity increase. Autonomous systems can interact with their surroundings in ways that were not fully anticipated during testing, particularly when they learn from new data or interact with other automated systems. These factors strengthen, rather than weaken, the State's obligation to impose operational limits, monitoring arrangements, and mechanisms for timely human intervention.

Some States may seek to invoke force majeure to avoid responsibility for unexpected decisions made by autonomous systems, including attacks on civilians. Such a defence should not be accepted where the harmful event resulted from defective programming, inadequate testing, negligent maintenance, insufficient cybersecurity, or deployment in an environment exceeding the system's demonstrated capabilities.⁴⁸⁴⁹

Under Article 23 of the Articles on Responsibility of States for Internationally Wrongful Acts, force majeure requires an irresistible force or an unforeseen event beyond the control of the State that makes performance of the obligation materially impossible. The defence does not apply where the situation is attributable, alone or in combination with other factors, to the conduct of the State invoking it, or where the State assumed the risk of the situation arising.

Physical impossibility may arise from events such as extreme weather, earthquakes, floods, or other external circumstances that genuinely remove State control. Ordinary technical malfunction does not automatically satisfy this standard. Weapons of every type may malfunction, and foreseeable system failure must be addressed through design, testing, maintenance, and operational safeguards.⁵⁰

A further difficulty concerns reparation for victims of violations. Civil proceedings may require victims to litigate in a foreign jurisdiction against a State or multinational manufacturer, often without adequate financial or technical resources. It is therefore inequitable to place the full burden of obtaining compensation upon those who have already suffered the harm.

The present legal gap concerning attribution and responsibility may facilitate impunity. Because autonomous weapon systems lack moral agency and legal personality, responsibility cannot properly be transferred to the machine. The State that develops, acquires, or deploys the system must remain responsible for violations resulting from its use where the applicable rules of attribution and breach are satisfied.⁵¹⁵²

State responsibility may also arise from failure to comply with Common Article 1 of the Geneva Conventions when developing or deploying systems whose operation is incompatible with international humanitarian law.⁵³ The duty to prevent harm begins during development and continues throughout testing, deployment, operation, maintenance, software modification, and withdrawal from service.

The absence of an effective mechanism for determining responsibility threatens to undermine the protective function of international humanitarian law. The emerging accountability gap cannot be addressed solely through post-hoc litigation. Preventive measures must therefore form a central part of the legal regime governing autonomous weapons.

The international community, acting through the United Nations, intergovernmental organisations,

46 Marco Sassòli, "Autonomous Weapons and International Humanitarian Law," above, p. 149.

47 Michael Schmitt argues that humans and machines are governed by different standards and that the human actor must remain the starting point of responsibility. See Azhar Abd al-Amir Rahi Al-Fatlawi, *Responsibility of Developers of Autonomous Weapons under Public International Law* (Arab Center for Studies and Scientific Research, Egypt, 2021), p. 193.

48 Force majeure requires an irresistible or unforeseeable event beyond the State's control that makes performance materially impossible. See International Law Commission, *Yearbook 2001*, vol. II, Part Two, art. 23, commentary paras. 1–3.

49 Articles on Responsibility of States for Internationally Wrongful Acts (2001), art. 23.

50 Azhar Abd al-Amir Rahi Al-Fatlawi, *Responsibility of Developers of Autonomous Weapons under Public International Law*, above, p. 195.

51 A legal gap refers to the absence or incompleteness of a legal rule in circumstances requiring regulation. See Haider Adham Al-Ta'i, *Lectures on the Basic Principles of Legislative Drafting* (Baghdad, 2017), p. 18.

52 Azhar Abd al-Amir Rahi Al-Fatlawi, *Responsibility of Developers of Autonomous Weapons under Public International Law*, above, p. 196.

53 Common Article 1 of the four Geneva Conventions of 1949 provides that the High Contracting Parties undertake to respect and ensure respect for the Conventions in all circumstances.

and civil-society institutions, should work towards a binding instrument that prohibits or restricts the development and use of autonomous systems that cannot operate consistently with international humanitarian law or remain under meaningful human control.

The duty of due diligence in relation to autonomous weapons is comparable to the traditional international obligation of a State to exercise reasonable care to prevent harmful conduct occurring within its territory. Even where the State is not directly responsible for the acts of private individuals, it may incur international responsibility for failing to exercise reasonable diligence to prevent violations of international law.⁵⁴

Although relatively few treaties formulate this duty in express terms, judicial decisions and legal scholarship recognise the duty of prevention as a general principle of international law. A State must not knowingly allow its territory, infrastructure, or institutions to be used for acts contrary to the rights of other States. This is an obligation to employ appropriate means, not an absolute obligation to guarantee a successful outcome.^{55,56}

The Essen case before a British military court illustrates the consequences of failing to provide protection where German military personnel and an escort were convicted after failing to protect Allied prisoners of war from an attacking crowd.⁵⁷ By analogy, where a State negligently fails to maintain, update, or supervise an autonomous weapon and the system subsequently attacks protected persons or a diplomatic mission within its territory, State responsibility may arise from breach of the duty of prevention.

Recommendations

1. A dedicated international convention on autonomous weapon systems should be concluded. It should provide a clear definition of such systems, identify prohibited and restricted uses, and establish binding rules of accountability where violations occur.

2. Meaningful and effective human control should be required at every critical stage of weapon use, particularly during target identification, the decision to attack, and the termination or suspension of the system when unexpected consequences arise.

3. States should be required to conduct comprehensive legal and technical reviews of intelligent weapons before their development, acquisition, or deployment, in accordance with Article 36 of Additional Protocol I of 1977. The review should be repeated after every substantial software modification.

4. The legal responsibility of each actor in the chain of production and operation should be clearly determined, including the designer, programmer, manufacturer, operator, military commander, and deploying State. Responsibility should be assessed according to effective control, foreseeability of harm, and the capacity to prevent it.

5. Manufacturing companies should incur liability for defective intelligent products where the harm results from defects in design, programming, testing, or cybersecurity. Civil compensation alone should not be regarded as sufficient in cases involving gross negligence or prior knowledge of serious risks.

6. Intelligent systems should be required to retain reviewable technical records containing input data, machine decisions, human commands, and software updates. Such records are necessary to facilitate evidence gathering and the determination of responsibility after an incident.

7. Independent national bodies should be established to supervise high-risk artificial intelligence applications. Their functions should include licensing, technical inspection, and verification of safety, transparency, and legal compliance.

8. Artificial intelligence should not, at the present stage, be recognised as possessing independent criminal responsibility because it lacks legally recognised will and consciousness. Such recognition could permit the individuals, States, and companies exercising actual control to evade responsibility.

9. Force majeure or the alleged unpredictability of system behaviour should not be accepted automatically where the harm is connected to inadequate testing, negligent maintenance, defective programming, or deployment in an environment exceeding the system's demonstrated capabilities.

10. Effective international mechanisms should be created to compensate victims of autonomous weapon systems, including compensation funds or compulsory insurance schemes, so that injured persons

54 Muhammad Sami Abd al-Hamid, *The Law of War* (Dar Al-Matbu'at Al-Jami'iyya, Cairo, 2012), p. 375.

55 Ali Muhammad Kazim Al-Mousawi, *Direct Participation in Cyberattacks*, above, p. 175.

56 Du'a Jalil Hatim, "Autonomous Weapons and International Responsibility," above, p. 120.

57 Najat Ahmad Ahmad Ibrahim, *International Responsibility for Violations of International Humanitarian Law*, above, p. 293.

do not bear the full burden of litigating before foreign courts or against multinational companies.

References

I. Legal Instruments and Official Documents

The Four Geneva Conventions of 1949, Common Article 1.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), 1977, arts. 35(2), 36, and 91.

Federal Penal Code of the United Arab Emirates, Federal Law No. 3 of 1987, art. 56(4).

Iraqi Penal Code No. 111 of 1969, as amended, art. 42.

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, Yearbook of the International Law Commission, vol. II, Part Two (2001).

Articles on Responsibility of States for Internationally Wrongful Acts (2001), art. 23 (force majeure).

II. Arabic-Language Books and References

Abu Al-Wafa, Ahmad. International Law and International Relations. Cairo: Dar Al-Nahda Al-Arabiya for Publishing and Distribution, 2005. [In Arabic].

Al-Deeb, Abu Bakr Muhammad. Military Applications of Artificial Intelligence in Light of Public International Law. Egypt: Dar Al-Nahda Al-Arabiya, 2021. [In Arabic].

Al-Shafi'i, Hisham Omar Ahmad. International Responsibility for Damage Arising from Nuclear Space Activities. Egypt: Al-Dalil Company for Studies, Training, Printing and Publishing, 2013. [In Arabic].

Al-Sherbiny, Ahmad, and Wafaa Baghdadi. Internet Protection and Security: The Coming Challenge and Methods of Confrontation. Cairo: Egyptian General Book Organization, 2010. [In Arabic].

Al-Shawwa, Muhammad Sami. The Information Revolution and Its Implications for Criminal Law. Cairo: Dar Al-Nahda Al-Arabiya, 2003. [In Arabic].

Al-Shuraihi, Abd Al-Tawwab Mu'awwad. Lessons in Criminal Law: General Part. Faculty of Law, Zagazig University, 2017. [In Arabic].

Al-Ta'i, Haider Adham. Lectures on the Basic Principles of Legislative Drafting. Revised and expanded ed. Baghdad, 2017. [In Arabic].

Al-Azzawi, Salim Muhammad Radi'an. Producer Liability in Civil Laws and International Conventions. 1st ed., 2nd issue. Amman: Dar Al-Thaqafa for Publishing and Distribution, 2009. [In Arabic].

Al-Fatlawi, Azhar Abd Al-Amir Rahi. Responsibility of Developers of Autonomous Weapons under Public International Law. Egypt: Arab Center for Studies and Scientific Research, 2021. [In Arabic].

Al-Obaidi, Osama bin Ghanem. International Efforts to Combat Information Crime. Journal of Law, no. 39, Kuwait, 2015. [In Arabic].

Al-Mousawi, Ali Muhammad Kazim. Direct Participation in Cyberattacks. Beirut: Modern Book Institution, 2019. [In Arabic].

Amin, Muhammad Mahmoud. The Theory of the Internationally Wrongful Act: A Study in International Responsibility. PhD diss., College of Law, University of Baghdad, 2007. [In Arabic].

Ibrahim, Najat Ahmad Ahmad. International Responsibility for Violations of International Humanitarian Law. Alexandria: Mansha'at Al-Ma'arif, 2009. [In Arabic].

Salama, Safat Amin. Weapons of Future Wars: Between Imagination and Reality. United Arab Emirates: Emirates Center for Strategic Studies and Research, 2019. [In Arabic].

Sanad, Najati Sayyid Ahmad. Principles of the General Part of Criminal Law: Crime and Punishment. Faculty of Law, Zagazig University, 2011. [In Arabic].

Abd Al-Hamid, Muhammad Sami. The Law of War. Cairo: Dar Al-Matbu'at Al-Jami'iyya, 2012. [In Arabic].

Abd Al-Wahid, Anwar Mahmoud, and Ahmad Amin Abd Al-Majid. Robots between Imagination and Science. Cairo: Al-Ahram Center for Translation and Publishing, 2002. [In Arabic].

Issa, Haitham. The Pre-Contractual Duty to Explain through Artificial Intelligence Systems. Cairo: Dar Al-Nahda Al-Arabiya, 2018. [In Arabic].

Salah, Muhammad, and Ahmad Ahdi. *The Artificial Robot*. Egypt: Dar Al-Kutub Al-Ilmiyya for Publishing and Distribution, 2009. [In Arabic].

Wise, Edwin. *Robot Manufacturing Technology*. Egypt: Dar Al-Farouq for Cultural Investments, 2009. [Arabic translation].

Whitby, Blay. *Artificial Intelligence*. Translated by the Translation Department of Dar Al-Farouq. Egypt: Dar Al-Farouq for Cultural Investments, 2008. [Arabic translation].

III. Theses and Dissertations

Amin, Muhammad Mahmoud. *The Theory of the Internationally Wrongful Act: A Study in International Responsibility*. PhD diss., College of Law, University of Baghdad, 2007. [In Arabic].

Sa'awi, Celia. *Civil Liability of the Producer for Damage Caused by Defective Products*. Master's thesis, Faculty of Law and Political Science, University of Abderrahmane Mira, Algeria, 2017. [In Arabic].

Farhi, Hussein. *Civil Liability of the Producer*. Master's thesis, Faculty of Law and Political Science, Larbi Ben M'hidi University, Oum El Bouaghi, Algeria, 2014. [In Arabic].

IV. Arabic-Language Articles and Studies

Al-Obaidi, Osama bin Ghanem. "International Efforts to Combat Information Crime." *Journal of Law*, no. 39, Kuwait, 2015. [In Arabic].

Basal, Mahmoud Hijazi Mahmoud. "State Management of Legal Risks Associated with Space Activities." In *Proceedings of the Conference on Law and Technology*, Faculty of Law, Ain Shams University, Egypt, 2017. [In Arabic].

Ben Tria, Maamar. "The Concept of Product Defectiveness in the Producer's Civil Liability Regime and Insurance Solutions for Its Coverage: A Comparative Study." *Kuwait International Law School Journal*, 6th year, no. 22, Kuwait, 2018. [In Arabic].

Hatim, Du'a Jalil. "Autonomous Weapons and International Responsibility." *Journal of Legal Sciences*, special issue, Iraq, 2020. [In Arabic].

Harqous, Hamza. "A War without a Soul: Before the Robot Kills You." *Al-Akhbar*, Lebanon, 2018. [In Arabic].

Sassòli, Marco. "Autonomous Weapons and International Humanitarian Law: Advantages, Technical Questions, and Legal Issues Requiring Clarification." *Publication of the International Committee of the Red Cross*, Cairo, 2017. [Arabic edition].

Geiss, Robin. "Asymmetric Conflict Structures." *Selections from the International Review of the Red Cross*, vol. 88, no. 864, Cairo, 2006. [Arabic edition].

Hammes, T. X. "Fighting Robots: How Artificial Intelligence Will Change the Nature of Future Wars." *Future Center for Advanced Research and Studies*, 4 July 2017, accessed 22 November 2025. [Arabic publication].

V. Foreign-Language References

Hubbard, Patrick. "Sophisticated Robots: Balancing Liability, Regulation, and Innovation." *Florida Law Review* (2014).

Lin, Patrick, and Keith Abney. *Autonomous Military Robotics: Risk, Ethics, and Design*. San Luis Obispo, CA: California Polytechnic State University, 2008.

Marshall, Aarian, and Alex Davies. "Uber's Self-Driving Car Saw the Woman It Killed." *Wired*. Accessed 22 November 2025.

Hague Conference on Private International Law. *Convention on the Law Applicable to Products Liability*. Concluded 2 October 1973.

VI. Electronic Sources and Reports

Marshall, Aarian, and Alex Davies. "Uber's Self-Driving Car Saw the Woman It Killed." *Wired*. Accessed 22 November 2025.

Uber Communications. Official post concerning the suspension of autonomous-vehicle testing, X (formerly Twitter). Accessed 22 November 2025.

Hammes, T. X. "Fighting Robots: How Artificial Intelligence Will Change the Nature of Future Wars." *Future Center for Advanced Research and Studies*. Accessed 22 November 2025.