### **The Use of Artificial Intelligence in Armed Conflict under International Law**

*1 Faculty of Law, Universitas Lampung, Indonesia. E-mail: naeksiregar69@gmail.com*

*2 Faculty of Law, Universitas Indonesia, Indonesia. E-mail:*

*3 Faculty of Law, University of Debrecen, Hungary. E-mail:*

*4 Faculty of Law, Universitas Lampung, Indonesia. E-mail:*

**Abstract:** Artificial Intelligence (AI) is a technological achievement, simulating human intelligence through machines or computer programs. The integration of AI in military operations aims to minimize combatant casualties deployed as a defense tool in warfare. This is supported by characteristics that resemble human intelligence with higher effectiveness in completing work. Despite the advantages, concerns arise regarding the ideal implementation in armed conflicts due to potential security challenges. A significant issue lies in the legal perspective governing the role as a comprehensive defense tool. Therefore, this research aims to provide a descriptive analysis and examination of the regulatory framework surrounding AI in armed conflict. The results show that the absence of comprehensive regulations adds complexity to the accountability framework since determining liability becomes intricate, specifically when AI malfunctions due to substandard quality or improper use. In these instances, accountability may extend to both the creator and the user. The concept of liability is explained for violations in armed conflict according to international law, exploring the implications of liability and the associated responsibilities for the use of AI with legal principles.

**Keywords:** Artificial Intelligence, Armed Conflict, International Law.

# **Introduction**

Artificial Intelligence (AI) is the scientific and engineering discipline dedicated to crafting intelligent machines, primarily achieved through the use of computer programs. AI includes the emulation of human intelligence within machine processes and is focused on conceiving, constructing, and deploying computer systems.[[1]](#footnote-2) Furthermore, the technology shows the capability to execute tasks and address challenges at a level equivalent to human proficiency. Machines generated through AI present enhanced efficiency compared to conventional human methods. According to a 2019 survey, 37% of global organizations have integrated AI into operations. The use has increased significantly, with 89 countries experiencing a remarkable 270% increase over the past four years, including a tripling within a single year.[[2]](#footnote-3) AI was created to minimize the uncertainty and complexity of human behavior and replace with effective reasoning.

AI possesses several characteristics that merit careful consideration due to the relationship of the technology with the national security domain. Firstly, AI is a versatile technological paradigm with the potential for seamless integration into a myriad of applications. Secondly, numerous applications show dual-use capabilities, implying the applicability in military and civilian contexts. Image recognition algorithms can be trained for civilian purposes such as identifying individuals in YouTube videos while aiding the military in capturing terrorist activities through full-motion video (FMV). This type of FMV is acquired by Remotely Piloted Aircraft (RPA) deployed over regions such as Syria or Afghanistan. Additionally, the deployment of AI in armed conflicts is exemplified by the implementation of Lethal Autonomous Weapons Systems (LAWS) in Israel. Thirdly, a level of transparency is shown that may not be immediately discernible on integration into a product. The presence represents the potential to address various challenges, with an expectation that AI will become an integral component in diverse applications, including defense technology. AI plays an important role in problem-solving across a spectrum of activities, solidifying the multifaceted landscape of technological advancements.

Military organizations are still trying to develop application technologies or concepts of war. The use of AI in armed conflict is considered to provide an advantage because the technology is different from conventional weapons with immediate countermeasures.[[3]](#footnote-4) This can be seen in intellectual, logistics, cyberspace, control, and automated vehicles. Even though different breakthroughs have been experienced, the development of military AI technology is in the early stages. Based on research, the use of AI in armed conflict is very risky in terms of security. Current security issues will not be solved by AI making the technology inadvisable for military use. This concern is evident in the deployment of AI LAWS, a contentious military application due to the capability to autonomously engage and eliminate targets without direct human intervention.[[4]](#footnote-5) LAWS as a form of AI used in armed conflict certainly causes unwanted casualties and violates the principles of laws of war. This weapon can identify and select targets as well as apply force to opponents without human intervention.[[5]](#footnote-6) An example of the use of LAWS is the Israeli Harpy Loitering Weapon, owned by the State of Israel. The weapon can detect, attack, and destroy enemy radar transmitters and conceal torpedo mines that release a torpedo to lock onto a target when activated by a ship.[[6]](#footnote-7)

The incorporation of AI in armed conflict shows a disparity between the increased intensity of military advancements and the susceptibility of society to the inherent risks. This gap has prompted a pressing need for strong protective measures. Safeguarding the use of AI is a complex challenge, primarily due to the diverse perspectives from which the regulation can be approached. The absence of international framework that comprehensively acknowledges AI as a tool for defense complicates matters. Currently, AI has obtained attention primarily in the context of intellectual property laws, affording protection to inventions, as opposed to being regulated by humanitarian and war laws.[[7]](#footnote-8) The use is also challenging because AI can cause fatal damage and liability must be applied when the damage results in casualties. However, the application of AI liability may be difficult because the status is only an indirect object. Liability for offenses is ambiguous because malfunctions can occur intentionally or unintentionally based on a failed product or user negligence. Therefore, the research aims to examine the regulation of the use of AI and the concept of liability for violations caused through a research entitled, "The Use of AI in Armed Conflict under International Law".

# Based on the background explanation, the questions raised are **"How is the regulation of AI in armed conflict according to international law?"** and **"How is the concept of responsibility for violations in the use of AI in armed conflict according to international law?"**.

# **Method**

In the normative legal research, principles, systematics, and comparisons were analyzed. Based on the nature, the normative research describes data in detail to find facts, identify problems, and discuss problems.[[8]](#footnote-9) The problem approach in a thesis refers to the series of steps carried out in the process of problem-solving.[[9]](#footnote-10) This stage mainly determines the approach under the problem formulation to fulfill the research objectives. The stage continues by identifying the subject matter of the problem formulation. In the subject matter, the problem approach determines the details of the sub-problems. The examination of the issue is subjected to a systematic process including the collection, processing, and analysis of data. The problem approach is completed by describing the discussion of the results and conclusions answering the formulation of the problem.

# **Discussion**

# **Regulation of AI in Armed Conflict Under International Law**

* + 1. **Regulation of AI Under International Law**

Article 19 of the Universal Declaration of Human Rights (UDHR) asserts, "Everyone has the right to freedom of opinion and expression, and this right includes freedom to hold opinions without interference, receive and impart ideas through media and frontiers." The important query arises: How can freedom of expression be upheld when public opinion is subject to influence by AI? The advent of these new tools introduces novel challenges to the preservation of freedom. Even though innovative tools are provided for content creation, including audio and visual analytics, the impact on freedom of expression is refined. AI has the potential to support the foundational principles of democracy and counteract corruption by enhancing freedom of expression. Striking a balance that safeguards freedom of expression while mitigating the risks posed by AI's influence on public opinion remains a challenge.[[10]](#footnote-12) The systems found in social media are also used to influence public opinion and to guide social movements by considering workflow optimization, automated content generation, content generation from old archives, content selection to target audience demographics, asset selection optimization, metadata generation, and content personalization. AI can personalize, generate, and filter content. This has implications for freedom of expression, social movements, and election campaigns. Questions arise regarding unreliable or false information published by the media but selected and continues to trend by AI.[[11]](#footnote-13) How can the level of trust be determined in media manipulated by governments, advertisers, algorithms, or other third parties trying to persuade users and recipients of information? Some AI systems are more efficient than humans at certain tasks such as mimicking the voices and images of others to influence people and create political change. Meanwhile, there is also the concept of machine learning software creating fake videos. The innovative technology by the Chinese tech giant Baidu has the capability to replicate a convincing artificial voice using 3.7 seconds of audio. Similarly, the concept extends to machine learning software, which has the potential to generate deceptive videos. In the same context, Montreal-based AI startup Lyrebird claims to be able to perform text-to-speech with one minute of audio.[[12]](#footnote-14)

According to Article 12 of the Universal Declaration of Human Rights, "No individual shall be subjected to arbitrary interference with privacy, family, home or correspondence, or attacks on honor and reputation." However, a system that combines data from satellite imagery, facial recognition-powered cameras, and cell phone location information can provide an individual's movements. This technology can easily be used to facilitate more precise restrictions on freedom of movement at the individual and group levels as well as by foreign actors targeting political change. Voting behavior and election campaigns are also influenced by social media. The continuous connection to smartphones greatly aids in the swift identification of every COVID-19 case, contributing to the mitigation of the impact and scale of the pandemic. The current smartphones even allow remote access to electro-grams. This creates new risks and challenges ranging from privacy to freedom of expression, given the tension between individuals and governments regarding human rights and democracy. The program of facial recognition raises privacy concerns that give rise to a digital dictatorship. In contrast, "the facial recognition market is expected to grow to US$7.7 billion by 2022 from US$4 billion in 2017”. Facial recognition technology finds diverse commercial applications, spanning from surveillance to marketing. The convergence of COVID-19 and AI is propelling societies into a new historical phase, marked by the growing use of robots for online shopping and delivery, digital and contactless payments, remote working, and distance learning. According to the OECD, AI is a transformative force, reshaping lives and impacting various sectors.[[13]](#footnote-15)

In this context, digital technology can play a role in contact tracing programs implemented in member states. Some countries are using AI to ensure access to information and track COVID-19 but the applications also track individuals.[[14]](#footnote-16) Under International Health Regulations, Member States bear the obligation to establish public health surveillance systems that effectively capture data essential for the response to COVID-19. These systems must maintain transparency, and responsiveness to public concerns, as well as refrain from imposing unwarranted burdens, such as the invasion of privacy. AI creates new challenges for international human rights law and can be a risk to freedom and privacy. According to the World Health Organization, "the use of the data could also threaten human rights and fundamental freedoms during and after COVID-19 pandemic. Furthermore, the blurred line can be quickly crossed between disease and population surveillance". Free and open scientific data provides another challenge that requires rethinking international law with new ideas related to the state and sovereignty. Open access to scientific data creates new risks to data sovereignty, causing conflict between China and the US. Donald Trump and the administration have accused China of failing to share COVID-19 samples with other countries. The cause of conflict is data sovereignty essential for technological sovereignty. In the era of AI, data sovereignty is a fundamental prerequisite for asserting and maintaining sovereignty.[[15]](#footnote-17)

In 2019, the Council of Europe established the Ad Hoc Committee on AI (CAHAI) working on "the feasibility and potential elements based on extensive multi-stakeholder consultations, of a legal framework for the development, design, and application of AI, based on Council of Europe standards on human rights, democracy and rule of law". Several international organizations are working on rules and legal frameworks related to ethics, such as the European Commission's High-Level Expert Group on AI (AI HLEG), which produced DRAFT Ethical Guidelines for Trustworthy AI. According to the draft of ethical guidelines prepared by AI HLEG, "objectives are used to show the development, application, and use of AI that ensures compliance with fundamental rights and applicable regulations, as well as respect for core principles and values. This is one of the two core elements for achieving Trustworthy AI".[[16]](#footnote-18) The initiative aims to prepare European countries for the tangible and intangible impacts of AI, including socio-economic changes, an objective conditioned by European values and guaranteed by an ethical and legal framework. Fundamental legal reforms and new policy actions that include the integration of stakeholders are required. The European Union is based on a constitutional commitment to protect the fundamental and indivisible rights of human beings as cited in Articles 2 and 3 of the Treaty on European Union and the Charter of Fundamental Rights of the European Union. The ethics in AI are reflected in the statement of principles, values, and rights.[[17]](#footnote-19)

The foundation lies in trust, serving as the bedrock safeguarding human rights in the age of AI. Despite the acceleration of the adoption across various sectors due to COVID-19 pandemic, including healthcare, manufacturing, and aviation, the increased use of AI has also exposed humanity to new threats concerning the security of the systems. The increasing significance and influence of data science in enhancing confidence in AI are essential in the battle against COVID-19. Additional global and regional frameworks focus on the application of AI with a human-centered approach. For instance, G20 AI Principles, adopted by the Ministers of Trade and Digital Economy in June 2019, draw inspiration from OECD recommendations on AI. The objective is to integrate a human-centric perspective into AI, representing the sole means to ensure human rights and democracy in AI era. According to the principles, trust in AI stands at the forefront and necessitates contributions from all stakeholders. Trust is shown as the primary principle, serving as the cornerstone for upholding human rights, democracy, and sustainable development. As articulated in the principle, AI actors must adhere to the rule of law, human rights, and democratic values throughout the life cycle of the systems. These include freedom, dignity, autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognized labor rights.[[18]](#footnote-20)

The document is a call to action and contains recommendations that require the inclusion of all stakeholders. Part of the document is dedicated to solutions and policy actions adopted by different countries and shows the importance of international cooperation. A more contemporary example of ethical principles is the G7 (2018) Charlevoix Common Vision for the Future of AI, ratified in Charlevoix, Canada, in June 2018 by the leaders of Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. This set of principles comprises 12 commitments and AI relies on a steady policy environment to nurture innovation.[[19]](#footnote-21) Several actions are recommended to member states based on an "ethical and technologically neutral approach" as stated in the first commitment of vision. The latest examples of such guidelines include the declaration by the African Union Working Group on AI, which Sharm El Sheik declared as adopted by African ministers responsible for communications and information and technologies (CICT) in Egypt on October 26, 2019. This important legal framework confirms that international community is dedicated to the importance of ethics in AI, including the development of rules and strategic measures to face the challenges imposed by AI and the importance of updating international law.

Directly, AI generates new legal situations by creating new entities or by enabling new behaviors. Indirectly, the technology can shift incentives or values for states interacting with international law. Therefore, three types of legal effects affected by disruptive technology can be distinguished. The first is legal development, comprising elemental changes that lead to the need for legal change to accommodate or address new situations. The second is legal displacement, which includes the systemic substitution of regulatory modalities, and 'automation' of international law. Meanwhile, the third is legal destruction, constituting systemic disruption of key venues and erosion. These legal effects are examined to understand the conditions under which AI may result in manageable development or change.[[20]](#footnote-23)

Technology creates an immediate need for new sui generis rules to deal with situations or forms of behavior.[[21]](#footnote-25) AI enables new forms of behavior that are morally problematic or politically or strategically disruptive. This includes systematic monitoring and control of populations through enhanced surveillance, deployment of fully autonomous weapons, and tracking of rival nuclear assets in ways that threaten deterrence stability. The behavior may be considered dangerous and undesirable, creating the need and conditions for new treaties to explicitly prohibit or control the development, deployment, or use of the systems. In the context of international law, this may echo past arms control efforts, such as the 1968 Treaty on the Non-Proliferation of Nuclear Weapons or the 1972 Treaty on the Limitation of Anti-Ballistic Missile Systems. Even though the establishment of new technology-specific treaty regimes to address gaps is not politically easy, international legal system is capable of proposing and disseminating new legal regimes to address gaps opened by new technologies.

Technology creates uncertainty about the application of new behavior to existing law. This includes uncertainty in the classification of new activities, entities, or relationships because there is no adequate classification. Therefore, there is an increased need to clarify and shape the existing legal rules. Matthew Scherer argues that the autonomy, and opacity of certain AI systems can create uncertainty over attribution, control, and responsibility. According to Thomas Burri, the case law of international courts, such as International Tribunal for the Former Yugoslavia or International Court of Justice (ICJ), includes more than enough precedents to resolve issues of state control, attribution, and delegation limits. Even though judicial clarifications are not available, new legislation, treaties, or customary international law can close the gap to provide the necessary conceptual clarifications surrounding AI system.[[22]](#footnote-27)

The new technologies create a new context that leads to inclusiveness and over-inclusiveness of laws. Previously unproblematic laws are suddenly found to have an inappropriate scope. For example, some arguments are completely on legal grounds rather than ethical or philosophical to give certain algorithms a semblance of personality. Shawn Bayern argued that a loophole in existing US corporate law might allow the incorporation of the limited liability company (LLC) under the operational control of AI system. The LLC is left with the algorithm fully and solely in charge when other members step down, functionally establishing AI entity with personality. Even though courts were reported not to interpret the relevant legislation, the result was contrary to legislative intent. This was because Bayern and others extended the argument to the German, Swiss, and English legal systems.[[23]](#footnote-28) According to Burri, when establishing these entities within an EU member state, the internal market principle of mutual recognition of national legal personality dictates that these entities should be acknowledged by all member states of the EU. This is stated in the European Court of Justice decisions in Centros Ltd v Erhvervs-og Selskabsstyrelsen and Berseering BV v Nordic Construction Company Baumanagement GmbH. The legal means or exploitation to establish AI personhood creates the potential for criminal abuse and inclusiveness of existing laws where the gap should be patched through judicial review or legislation.[[24]](#footnote-29)

In the following discussion, the legal review of AWS is based on international treaty, whose provisions are considered to be closest to the characteristics of AWS, namely the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (the 1980 Conventional Weapons Convention). In the 1980 Conventional Weapons Convention, there was general agreement among state parties that "meaningful" or "effective" human control or supervision, or an "appropriate level of human judgment" must be maintained on the use of a weapon system to meet legal and ethical requirements. This is certainly difficult to fulfill by the characteristics of AWS because human inclusion is limited to the development and activation stages. Meanwhile, the operation stage of AWS does not require human intervention, and this results in a real threat when there is a failure in the operating system.

As explained earlier, legal review can also be based on the Martens Clause contained in the Preamble of Hague Convention IV respecting Laws and Customs of War on Land (Convention IV Den Hagg 1907), which reads as follows:[[25]](#footnote-30)

*“Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the adopted Regulations, populations, and belligerents remain under the protection and empire of the principles of international law, resulting from the usages established between civilized nations. This is related to the laws of humanity and the requirements of the public conscience.”*

Based on the provisions, the Martens Clause is intended for events or problems not regulated in the provisions of International Humanitarian Law. Therefore, when there is a void or gap in positive law, the solution taken must be based on basic humanitarian principles and general awareness.[[26]](#footnote-31) The purpose of the clause is to prevent the possibility of leaving unregulated matters to the arbitrary opinion of commanders. The principle of humanity requires humane treatment of other individuals and respect for life and dignity. Due to these characteristics, AWS neglects to uphold human dignity by relying on algorithmic calculations embedded in computer systems for determining matters related to human life and death, as well as targeting attack objectives. The characteristics also run counter to common sense since AWS incorporates the concept of a weapon system that executes the use of force and attacks beyond human control.

* + 1. **AI in Armed Conflict**

International law has regulated the use of weapons in armed conflict as reported in the 1907 Hague Convention, where agreement was formed before the First World War. This regulation mentions the weapons and actions in armed conflict as stated in Article 23 of the convention. In this article, only two weapons are prohibited, namely, poisons and certain weapons, projectiles, or materials causing unnecessary suffering. [[27]](#footnote-32)

The use of "Agent Orange" by the United States Army in the Vietnam War is an example of a violation of Article 23 of the 1907 Hague Convention.[[28]](#footnote-33) "Agent Orange" was a toxic herbicide and defoliant weapon used to injure Vietnamese guerrillas. The civilians were also affected since the poison contaminated natural resources in conflict zone.

According to Article 23 of the 1907 Hague Convention, the use of AI Weapons in armed conflict is certainly not prohibited provided weapon is non-toxic and does not cause unnecessary or excessive suffering. For example, a drone that hits a military base automatically is a weapon with AI technology similar in nature to missiles. It is a weapon used to attack enemy bases without poison and does not cause unnecessary suffering. Even though the drone is AI weapon, no complain is stated since the provisions listed in the 1907 Hague Convention are not violated.

There is also a need for regulations governing the use of AI or autonomous weapon systems. Therefore, different regulations should be formed to control the use and restrictions of these weapons.

# **The Concept of Responsibility for Violations in the Use of AI in Armed Conflicts Under International Law**

#  **Implications of the Use of AI in Armed Conflicts**

AI weapons have destructive power useful for combating opponents but the impact may cause damage to civilian buildings and lives. For example, Israel's non-AI weapons have destroyed many civilians and buildings in Gaza. This violates the 1949 Geneva Convention, which provides for the protection of civilians and wounded soldiers.[[29]](#footnote-34) Therefore, AI or non-AI weapons constitute a violation after engaging in attacks against civilians and structures in compliance with the provisions outlined in the 1949 Geneva Convention. However, AI weapons have a higher potential and possibility to cause massive and fatal destruction. A regulation useful for limiting the use and development of these weapons is necessary to prevent the destructive power.

* + 1. **Command Responsibility for the Use of AI in Armed Conflicts**

Commanders of the army are responsible for the performance of the forces subject to authority. In US joint force doctrine, the term "command" includes the authority and responsibility to organize, direct, coordinate, and control military forces to accomplish the mission. Furthermore, it includes responsibility for the health, welfare, morale, and discipline of all subordinates. The art of command flows from the commander's ability to use leadership to maximize performance. "The clear guidance and intentions, enriched by experience and intuition, enable the joint force to achieve different objectives.”.[[30]](#footnote-35) Historically, the most senior military officers are held responsible for the general performance of troops in combat. Commanders lead through a combination of "courage, ethical leadership, judgment, intuition, situational awareness, and the capacity to consider conflicting views...." In the Navy, these individuals are required to adhere to the principles of international law. To fulfill the responsibility, there is authorization to enforce international law when conflict exists between international and other Navy regulations. The Hague Regulations require commanders to be directly or individually responsible for the methods of warfare during hostilities. American commanders must devise appropriate rules of engagement to accomplish the mission. Obedience is the cornerstone of military discipline, and while subordinates are subject only to law, all orders are presumed valid unless the presumption is rebutted. This accountability has always been an inherent element of US military leadership. Penalties for LOAC violations fall on individuals for acts committed under orders.

Commanders bear the weight of responsibility for battlefield actions, irrespective of whether subordinates make and amplify mistakes, machines deviate unexpectedly, or incidents unfold as unforeseen consequences of pure chance or the complexities inherent in the fog of war.[[31]](#footnote-36) The military doctrine of command accountability may not look "fair" because the commander is responsible for every decision made throughout armed forces and the prosecution of the war effort. Direct accountability includes every aspect of the outcome of specific decisions made by subordinate leaders and service members, failures of intelligence and mission analysis, mistakes of the government and civilian private sector accompanying forces, and faulty weapons performance. Meanwhile, the military commander is responsible for the totality of the use of the forces, from the gun to the nuclear missile. In this context, criminal, non-judicial, and administrative liability are faced. The direct liability for almost every attempt at prosecuting war is a strict regime without criminal sanctions. Even though the responsibility may comprise legal disclosure of criminal violations of laws related to warfare, non-judicial and non-legal mechanisms are included in military doctrine. Liability is separate and distinct from the related legal doctrine in international criminal law of command responsibility. The commanders can face legal jeopardy for failure to exercise control over forces under command in violation of LOAC. Meanwhile, lethal force is authorized against enemies and lawful targets under the rules of engagement and subject to LOAC.

These orders are informed by the understanding of the tactical situation, training and experience, and the combination of tactics and weapons. In the case of AI, commanders are responsible for calibrating the use of AWS, "express autonomy", and setting parameters or "guardrails" for operations. The military system holds the commander accountable for failing to anticipate or guard against harm when an autonomous system acts outside its programmed boundaries. The leaders in command have the authority to deploy weapons and bear responsibility when the machinery malfunctions. These individuals are answerable to superiors in the chain of command for the strategies and tools of war initiated, ranging from missiles in flight to artillery shells discharged from tubes. The accountability extends to AWS, capable of locating targets based on programmed criteria. Commanders are held accountable for instances such as troops firing incorrect or misdirected rounds, weapons failing to perform as anticipated, and errors occurring across the entire kill chain when using systems with autonomous functionalities. This accountability includes both criminal and administrative liability, where personal exposure or responsibility is assumed for the weapons discharged and may face sanctions for violations of laws. The pursuit of advances in weapon systems to ensure an effective, efficient, and more humane approach to warfare has been successful due to the coupling with a culture of accountability in battlefield leadership.

The concept of command responsibility in Additional Protocol I of the Geneva Convention 1977 is regulated in Article 86 paragraph (2) AP stating that after the commission of an offense by a subordinate, the superior or commander remains subject to potential repercussions. The command structure should possess knowledge or information regarding the likelihood of subordinates engaging in misconduct, necessitating the implementation of measures to prevent or suppress such offenses.

The provisions in Article 28 letter (a) of the Rome Statute states that:

“*The fact a breach of the conventions or this Protocol was committed by a subordinate does not absolve his superiors from penal or disciplinary, as the case may be, if they knew, or had information which should have enabled them to conclude in the circumstances at the time, that he was committing or was going to commit such a breach and if they did not all feasible measures within their power to prevent or repress the breach*.”

The unaddressed aspects of the relationship between superiors and subordinates are explained in Article 28, letter (b) of the Rome Statute. Based on the provisions of Article 86 paragraph (2) AP I Geneva Convention 1977 jo., Article 28 letter (a) Rome Statute jo., and Article 28 letter (b) of the Rome Statute, the elements of command responsibility are:

1. There must be a relationship between the commander and the subordinate reasonably suspected of committing a crime. The phrase "relationship" refers to the meaning that the command and subordinate have a common duty in a military environment. The relationship is vertical with the commander as a senior and the subordinate as a junior in the environment.
2. The commander in question actually and effectively exercised effective command or supervision over the subordinate suspected of committing the crime. Effective supervision by a commanding officer over subordinates includes the tangible capacity to prevent criminal activities by subordinates. This comprises the material ability to hinder subordinates from engaging in criminal behavior and proactive measures such as the capability of the commanding officer to promptly report the matter to the appropriate authorities.
3. The commander's awareness or reasonable expectation that subordinates have perpetrated a criminal act is crucial. According to the provisions of International Criminal Court (ICC) concerning the expression "a commander knew or should have known," this criterion is expected to be included in the future and requisite for establishment during trial. The assertion is that the commander neglected to conduct logical and essential measures to address or transfer the issue to an authorized official capable of conducting further inquiries. Therefore, this leader will be characterized as having failed to exercise control over subordinates, leading to the commission of the crime.
	* 1. **The Concept of Responsibility for the Use of AI in Armed Conflict Under International Law**

Legal responsibility for the actions of AI needs to be researched properly. Even though AI has the same legal subject position as Legal Entities, the responsibility for acts committed must be clear with certainty. The responsibility must be borne by User as well as the Legal Entity as the person in charge is the director of the company or the head of the foundation. However, the person in charge is not only limited to the User, there are still important parties that should not be ruled out, namely the Creator. The creator is the one who makes AI adopted by Users, the algorithm system, the database, and the design. This individual must be responsible for the legal actions carried out by AI created. The users are affected when there is an error in creation or intentionality to destroy without the awareness of unfamiliar individuals. The accountability arrangements will be impacted when the use of AWS contradicts the provisions of International Humanitarian Law. There are 2 (two) forms of responsibility in International Law, namely:

1. State Responsibility

State responsibility will arise when there are state actions that violate obligations in International Law, as stated in Article 1 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts (**Draft Convention on State Responsibility**) "Every internationally wrongful act of a State includes the responsibility." A total of 2 forms of International Law can be violated, namely: (1) public international law based on treaties, customary, and principles of international law, as well as (2) bilateral or multilateral treaties.

Concerning state action, Article 8 of the Draft Convention on State Responsibility mentions that:

“*The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.”*

The article provides that when a person or group of people acts at the instruction or under the direction or control of the state, then the action is considered a state action. A more specific provision is stated in Article 4 of the Draft Convention on State Responsibility. This article specifies that an action falling within the state includes the organ that possesses the authority to act. An example of such an organ is armed forces of a state. Based on these provisions, when armed forces are mobilized to carry out an attack using AWS, and there are errors and violations of International Humanitarian Law, then the state can be held internationally accountable.

1. Individual Responsibility

Several parties can be held individually responsible for the misuse of AWS, namely: (1) combatants, (2) military commanders, (3) programmers, and (4) AWS designers. The discussion of individual liability is limited to International Humanitarian Law, and the parties to be discussed are combatants and military commanders. In International Humanitarian Law, individual responsibility includes proving mental and physical elements. Provisions regarding mental elements are contained in Article 30 of the Rome Statute of International Criminal Court (Rome Statute 1998), constituting intent and knowledge. Intent refers to an individual's deliberate intention to participate in the commission of an offense and bring about the associated consequences. Meanwhile, knowledge is the individual's awareness of the offense or the consequences that will occur. Based on Article 25 paragraph (3) of the 1988 Rome Statute, criminal acts must fulfill the elements of the crime. An individual must be held responsible when proven to fulfill mental and physical elements of a criminal offense.

# **Conclusion**

In conclusion, there was no specific regulation of AI in international humanitarian law. Therefore, a special arrangement was needed to provide limits rather than prohibit the development of excessive weapons. The use of autonomous weapons, which could operate independently without human intervention, might not inherently include the principles of indiscriminateness, distinction, military necessity, and proportionality. However, the humanity principle was also considered since the state as a subject of international law could be held accountable for the use of AI. Accountability by the commander as an order giver was still a problem because of the difficulty in proving the element of violation. Normatively, a clear relationship existed between the commander and subordinates as armed forces of a country. Establishing the element of guilt posed challenges due to the non-moral agency nature of AI, which lacked a hierarchical relationship of the superior-subordinate dynamics inherent in conventional soldiers. Therefore, the regulation of AI was crafted to ensure the usage was in line with established procedures within the framework of international law.

# **Suggestion**

1. As stated in the discussion, the singular regulation addressing the use of weapons in armed conflict is the 1907 Hague Convention. However, this convention primarily focuses on specific weaponry and is excessively broad. In the contemporary landscape, numerous nations have advanced the development of weapons incorporating AI technology. To prevent the production of exceedingly negative AI weapons and safeguard human life, it is important to institute a regulation that explicitly governs the manufacture and progression.
2. Individuals responsible for the use of AI or autonomous weapon systems include combatants, military commanders, programmers, and designers. In practice, there are difficulties in identifying the perpetrator controlling the autonomous weapon system. Therefore, there is a need for regulations where each AI weapon has an identity with the person in charge. This is useful to facilitate accountability when there is a violation of international humanitarian law.

**References**

Allam, Zaheer, and Zaynah A Dhunny, “On Big Data, Artificial Intelligence and Smart Cities.” *Cities* 89 (2019): 80-91, https://doi.org/10.1016/j.cities.2019.01.032.

Anugerah, Julian Tommi, “Tanggung Jawab Negara pada Penggunaan Senjata Kimia Saat Perang (Tinjauan Kasus : Agent Orange 1954 – 1975).” *Jurist-Diction* 2, no. 2 (2019): 523.

Badan Siber dan Sandi Negara. “Pembentukan Badan Siber Dan Sandi Negara.” <https://www.bssn.go.id/pembentukan-badan-siber-dan-sandi-negara-bssn/> (accessed May 30, 2023).

Boulanin, Vincent, Laura Bruun, and Netta Goussac, *Autonomous Weapon Systems And International Humanitarian Law: Identifying Limits and the Required Type and Degree of Human–Machine Interaction* (Stockholm: Stockholm International Peace Research Institute, 2021).

De Sousa, Weslei Gomes, et al., “How and Where is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda.” *Government Information Quarterly* 36 no. 4 (2019): 1-8, https://doi.org/10.1016/j.giq.2019.07.004.

De Spiegeleire, Stephan, Matthijs Maas, and Tim Sweijs, *Artificial Intelligence and The Future of Defense Strategic: Implications for Small- and Medium-Sized Force Providers* (Den Haag: Hague Centre for Strategic Studies, 2017), 2-5.

Farrow, Elissa, “To Augment Human Capacity — Artificial Intelligence Evolution Through Causal Layered Analysis.” *Futures* 108 (2019): 61-71, https://doi.org/10.1016/j.futures.2019.02.022.

Goralski, Margaret A., and Tay Keong Tan, “The International Journal of Artificial Intelligence and Sustainable Development.” *The International Journal of Management Education* 18 no. 1 (2020): 1-9, https://doi.org/10.1016/j.ijme.2019.100330.

Guevarrato, Gulfino, Ida Bagus Oka Ana, and Budi Gautama Arundhati, “Analisis Hukum Konflik Bersenjata Antara Palestina dan Israel dari Sudut Pandang Hukum Humaniter Internasional.” *Artikel Ilmiah Hasil Penelitian Mahasiswa* 1 no. 1 (2014): 6, http://repository.unej.ac.id/handle/123456789/56147.

Haenlein, Michael, and Andreas Kaplan, “A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence.” *California Management Review* 00 no. 0 (2019): 1, 10.1177/0008125619864925.

Hoadley, Daniel S., and Nathan J. Lucas, *Artificial Intelligence and National Security* (Washington D. C.: Congressional Research Service, 2018).

Kandhro, Sirajul Haque, “Roles of E-Government in Enhancing Good Governance of Public Sector Organizations in Pakistan.” *National Institute of Development Administration* (2011): 9-61, 10.14457/NIDA.the.2011.78.

Kusumo, Ayub Torry Satriyo, and Kukuh Tejomurti, “Alternatif atas Pemberlakuan Hukum Humaniter Internasional dalam Konflik Bersenjata Melawan Islamic State of Iraq and Syria” *YUSTISIA* 4 no. 3 (2015): 654, https://doi.org/10.20961/yustisia.v4i3.8696.

Moşteanu, Narcisa Roxana, and Kevin Galea, “Artificial Intelligence and Cyber Security - Face to Face with Cyber Attack a Maltese Case of Risk Management Approach.” *ECOFORUM*  9 no. 2(22) (2020): 1-8.

Muhammad, Abdulkadir, *Hukum dan Penelitian Hukum* (Bandung: PT Citra Aditya Bakti, 2004).

Pedron, Stephanie Mae, and Jose de Arimateia da Cruz, “The Future of Wars: Artificial Intelligence (AI) and Lethal Autonomous Weapon Systems (LAWS).” *International Journal of Security Studies* 2 no. 1 (2020): 4, 10.31945/iprij.220105.

Petit, Nikolas, “Law and Regulation of Artificial Intelligence and Robots: Conceptual Framework and Normative Implication.” *Working Paper* (2017): 1, http://dx.doi.org/10.2139/ssrn.2931339.

Romagna, Marco, and Niek Jan Van Den Hout, “Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats.” *Virus Bulletin Conference* (2017), 1-8.

Sethu, Sagee Geetha, “The Inevitability of an International Regulatory Framework for Artificial Intelligence.” International Conference on Automation, Computational, and Technology Management (ICACTM) (2019): 367, 10.1109/ICACTM.2019.8776819.

Sharma, Gagan Deep, Anshita Yadav, and Ritika Chopra, “Artificial Intelligence and Effective Governance : A Review, Critique and Research Agenda.” *Sustainable Future* (2019): 0– 5, https://doi.org/10.1016/j.sftr.2019.100004.

Sidauruk, Sarah Marisi Ireney, Nuswantoro Dwiwarno, and H.M. Kabul Supriyadhie, “Penggunaan Autonomous Weapons System Dalam Konflik Bersenjata Internasional Menurut Hukum Humaniter Internasional.” *Diponegoro Law Journal* 8 no. 2 (2019): 1489–1505, https://doi.org/10.14710/dlj.2019.25474.

Soekanto, Soerjono, *Pengantar Penelitian Hukum* (Jakarta: Penerbit Universitas Indonesia, 2012).

Sulistia, Teguh, “Pengaturan Perang dan Konflik Bersenjata dalam Hukum Humaniter Internasional.” *Indonesian Journal of International Law* 3, no. 3 (2021): 530.

Trifonov, Roumen, Slavcho Manolov, and Radoslav Yoshinov, “Artificial Intelligence Methods for Cyber Threats Intelligence.” *International Journal for Computer* 2 (2017): 129–135.

Turlel, Y. Anastasya, “Perlindungan Penduduk Sipil Dalam Situasi Perang Menurut Konvensi Jenewa Tahun 1949.” *Lex Crimen* 6, no. 2 (2017): 147-148.

Vähäkainu, Petri, and Martti Lehto, “Artificial Intelligence in the Cyber Security Environment.” *Proceedings of the 14th International Conference on Cyber Warfare and Security ICCWS2019* (2019): 432-433.



1. Michael Haenlein, and Andreas Kaplan, “A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence.” *California Management Review* 00 no. 0 (2019): 1, 10.1177/0008125619864925. [↑](#footnote-ref-2)
2. Sagee Geetha Sethu, “The Inevitability of an International Regulatory Framework for Artificial Intelligence.” International Conference on Automation, Computational, and Technology Management (ICACTM) (2019): 367, 10.1109/ICACTM.2019.8776819. [↑](#footnote-ref-3)
3. Daniel S. Hoadley, and Nathan J. Lucas, *Artificial Intelligence and National Security* (Washington D. C.: Congressional Research Service, 2018), 36. [↑](#footnote-ref-4)
4. Stephanie Mae Pedron, and Jose de Arimateia da Cruz, “The Future of Wars: Artificial Intelligence (AI) and Lethal Autonomous Weapon Systems (LAWS).” *International Journal of Security Studies* 2 no. 1 (2020): 4, 10.31945/iprij.220105. [↑](#footnote-ref-5)
5. Vincent Boulanin, Laura Bruun, and Netta Goussac, *Autonomous Weapon Systems And International Humanitarian Law: Identifying Limits and the Required Type and Degree of Human–Machine Interaction* (Stockholm: Stockholm International Peace Research Institute, 2021), 1-52. [↑](#footnote-ref-6)
6. Sarah Marisi Ireney Sidauruk, Nuswantoro Dwiwarno, and H.M. Kabul Supriyadhie, “Penggunaan Autonomous Weapons System Dalam Konflik Bersenjata Internasional Menurut Hukum Humaniter Internasional.” *Diponegoro Law Journal* 8 no. 2 (2019): 1489–1505, https://doi.org/10.14710/dlj.2019.25474. [↑](#footnote-ref-7)
7. Nikolas Petit, “Law and Regulation of Artificial Intelligence and Robots: Conceptual Framework and Normative Implication.” *Working Paper* (2017): 1, http://dx.doi.org/10.2139/ssrn.2931339. [↑](#footnote-ref-8)
8. Soerjono Soekanto, *Pengantar Penelitian Hukum* (Jakarta: Penerbit Universitas Indonesia, 2012), 50. [↑](#footnote-ref-9)
9. Abdulkadir Muhammad, *Hukum dan Penelitian Hukum* (Bandung: PT Citra Aditya Bakti, 2004), 112. [↑](#footnote-ref-10)
10. Narcisa Roxana Moşteanu, and Kevin Galea, “Artificial Intelligence and Cyber Security - Face to Face with Cyber Attack a Maltese Case of Risk Management Approach.” *ECOFORUM*  9 no. 2(22) (2020): 1-8. [↑](#footnote-ref-12)
11. Stephan De Spiegeleire, Matthijs Maas, and Tim Sweijs, *Artificial Intelligence and The Future of Defense Strategic: Implications for Small- and Medium-Sized Force Providers* (Den Haag: Hague Centre for Strategic Studies, 2017), 2-5. [↑](#footnote-ref-13)
12. Marco Romagna, and Niek Jan Van Den Hout, “Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats.” *Virus Bulletin Conference* (2017), 1-8. [↑](#footnote-ref-14)
13. Gagan Deep Sharma, Anshita Yadav, and Ritika Chopra, “Artificial Intelligence and Effective Governance : A Review, Critique and Research Agenda.” *Sustainable Future* (2019): 0– 5, https://doi.org/10.1016/j.sftr.2019.100004. [↑](#footnote-ref-15)
14. Roumen Trifonov, Slavcho Manolov, and Radoslav Yoshinov, “Artificial Intelligence Methods for Cyber Threats Intelligence.” *International Journal for Computer* 2 (2017): 129–135. [↑](#footnote-ref-16)
15. *Ibid.* [↑](#footnote-ref-17)
16. *Ibid.* [↑](#footnote-ref-18)
17. Petri Vähäkainu, and Martti Lehto, “Artificial Intelligence in the Cyber Security Environment.” *Proceedings of the 14th International Conference on Cyber Warfare and Security ICCWS2019* (2019): 432-433. [↑](#footnote-ref-19)
18. *Ibid.* [↑](#footnote-ref-20)
19. *Ibid.* [↑](#footnote-ref-21)
20. Sirajul Haque Kandhro, “Roles of E-Government in Enhancing Good Governance of Public Sector Organizations in Pakistan.” *National Institute of Development Administration* (2011): 9-61, 10.14457/NIDA.the.2011.78. [↑](#footnote-ref-23)
21. Margaret A. Goralski, and Tay Keong Tan, “The International Journal of Artificial Intelligence and Sustainable Development.” *The International Journal of Management Education* 18 no. 1 (2020): 1-9, https://doi.org/10.1016/j.ijme.2019.100330. [↑](#footnote-ref-25)
22. *Ibid.* [↑](#footnote-ref-27)
23. Weslei Gomes de Sousa, et al., “How and Where is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda.” *Government Information Quarterly* 36 no. 4 (2019): 1-8, https://doi.org/10.1016/j.giq.2019.07.004. [↑](#footnote-ref-28)
24. Elissa Farrow, “To Augment Human Capacity — Artificial Intelligence Evolution Through Causal Layered Analysis.” *Futures* 108 (2019): 61-71, https://doi.org/10.1016/j.futures.2019.02.022. [↑](#footnote-ref-29)
25. Gulfino Guevarrato, Ida Bagus Oka Ana, and Budi Gautama Arundhati, “Analisis Hukum Konflik Bersenjata Antara Palestina dan Israel dari Sudut Pandang Hukum Humaniter Internasional.” *Artikel Ilmiah Hasil Penelitian Mahasiswa* 1 no. 1 (2014): 6, http://repository.unej.ac.id/handle/123456789/56147. [↑](#footnote-ref-30)
26. Ayub Torry Satriyo Kusumo, and Kukuh Tejomurti, “Alternatif atas Pemberlakuan Hukum Humaniter Internasional dalam Konflik Bersenjata Melawan Islamic State of Iraq and Syria” *YUSTISIA* 4 no. 3 (2015): 654, https://doi.org/10.20961/yustisia.v4i3.8696. [↑](#footnote-ref-31)
27. Teguh Sulistia, “Pengaturan Perang dan Konflik Bersenjata dalam Hukum Humaniter Internasional.” *Indonesian Journal of International Law* 3, no. 3 (2021): 530. [↑](#footnote-ref-32)
28. Julian Tommi Anugerah, “Tanggung Jawab Negara pada Penggunaan Senjata Kimia Saat Perang (Tinjauan Kasus: Agent Orange 1954 – 1975).” *Jurist-Diction* 2, no. 2 (2019): 523. [↑](#footnote-ref-33)
29. Y. Anastasya Turlel, “Perlindungan Penduduk Sipil Dalam Situasi Perang Menurut Konvensi Jenewa Tahun 1949.” *Lex Crimen* 6, no. 2 (2017): 147-148. [↑](#footnote-ref-34)
30. Badan Siber dan Sandi Negara. “Pembentukan Badan Siber Dan Sandi Negara.” <https://www.bssn.go.id/pembentukan-badan-siber-dan-sandi-negara-bssn/> (accessed May 30, 2023). [↑](#footnote-ref-35)
31. Zaheer Allam, and Zaynah A Dhunny, “On Big Data, Artificial Intelligence and Smart Cities.” *Cities* 89 (2019): 80-91, https://doi.org/10.1016/j.cities.2019.01.032. [↑](#footnote-ref-36)