Unity Journal
Vol.6, 34-47, Feb 2025
https://doi.org/10.3126/unityj.v6i1.75547
Prithvi Narayan Shah Research Center
Directorate General of Military Training, Nepali Army
Kathmandu, Nepal

ISSN - 2717-4751

Article history
Received: 10 Nov 2024
Accepted: 24 Jan 2025

Artificial Intelligence in Armed Conflict: Perspectives from International Humanitarian Law

Yatish Ojha[*]

Abstract

The use of artificial intelligence (AI) in armed conflict gives rise to unprecedented challenges in international humanitarian law (IHL). This article examines the complex relationship between AI and IHL. It focuses on the application of autonomous weapons systems (AWS), cyber warfare, surveillance, and precision targeting. The use of AI has been believed to enhance precision and reduce collateral damage. However, there are some challenges, like the loss of human control over decision-making, the potential for algorithmic bias, and the questions of attribution. These issues threaten the core principles of IHL, that is, distinction, proportionality, and humanity. This article finds that AWS, constituting a 'third revolution in military affairs, consists of a risk of violating the principle of distinction by misidentifying targets because of inherent biases in their programming. Similarly, the research discovers that the use of AI in cyber operations raises concerns about the proportionality of attacks and the difficulties in attributing responsibility for such operations. This article analyzes these challenges, including insights from case studies and comparative analyses of AI usage in military operations. The study follows a qualitative research methodology and analyzes data collected from primary and secondary sources. By exploring particular events, this research highlights the pressing need for a reconsideration of existing legal frameworks that address the peculiar challenges presented by evolving technology. Ultimately, this article seeks to contribute to the ongoing discourse on developing ethical and legal frameworks necessary to govern AI's use in warfare, ensuring compliance with IHL while respecting state sovereignty and national security.

Keywords: *Artificial intelligence, armed conflict, autonomous weapons, international humanitarian law, cyber warfare, national sovereignty*

Introduction

In October 2024, as the Royal Swedish Academy was announcing the Nobel Prize winners, internet users were joking that the prize in literature should be awarded to ChatGPT, a generative chatbot, "for its intricate tapestry of prose which showcases the redundancy of sentience in art" (ABP News Bureau, 2024). This came after the announcements that the Nobel prizes in Physics

[*] Law Graduate
Email ID : hrishyat@gmail.com

and Chemistry were awarded for contributions related to Artificial Intelligence (AI) (The Nobel Prize, 2024).

AI is one of the newest and rapidly growing fields in science and technology (Russell and Norvig, 2010). The concept of AI itself is not new. It came into existence in about the 1950s and 60s with the development of computers (Warwick, 2012). But the meaning and application of AI today, compared to the 50s and 60s, have significantly transformed. In 1950, the computer pioneer Alan Turing proposed an imitation game with the question, "Can a machine think?" popularly known as the 'Turing Test' (Suleyman & Bhaskar, 2023). This was a test for whether an AI exhibited human-level intelligence. Turing predicted that, within the year 2000, it would be possible to program computers to pass the test of imitating humans by at least 30% (Warwick, 2012).

In 1978, mathematician Richard Bellman defined AI as "the automation of activities that we associate with human thinking, activities such as decision-making, problem-solving, learning…" (Russell & Norvig, 2010). Since then, AI's capabilities have grown far beyond these early expectations.In 2001, programmers in Saint Petersburg developed perhaps the first chatbot to have a claim to passing the Turing Test (Mollick, 2024).Today, AI systems can perform a variety of tasks, including recognizing faces and objects, navigating roads and traffic to drive autonomously, generating images and text, producing synthetic voices, and composing music. It is also progressing in human capabilities like long-term planning, imagination, and simulation of complex ideas (Suleyman & Bhaskar, 2023). AI has evolved far beyond the Turing Test, from an experimental technology to a powerful tool in various sectors.

In parallel with technological developments, the nature of warfare has undergone significant transformations. There have been profound changes between the days of Greek gods of war, Ares and Enyo, or their Roman transformation, Mars and Bellona, and today. Etymologically, the root source for the English equivalent of war changed from the Latin word bellum to the German word werran, which became weorre and then warre, the obsolete spelling of war (Freedman, 2017). Men have been fighting in groups since the Stone Age, as depicted in cave art of 10,000 years ago. Mesopotamia and the city of Uruk are reported to have developed a military defense system and launched offensive military campaigns nearly 5,000 years ago (Solis, 2010). The Mahabharata, an oriental epic, which was written roughly 2,000 years ago, demonstrated conflicts in the Indian subcontinent.

Almost two millennia later, the First World War marked a distinct and terrifying break from the warfare of the past. A more efficient system of combined arms tactics of artillery, tanks, air, and infantry was developed along with the use of mobile infantry weapons such as light mortars, Lewis guns, and rifle grenades (Archer et al., 2002). Since then, the means and methods of warfare and the military strategies have advanced faster than ever. Some of the examples of warfare over the period of time range from the close-combat strategies of ancient empires to the organized tactics in the classical West. The refined techniques were seen in European chivalry and Islamic warfare. Subsequently, the industrial age saw the birth of mechanized and total war, which is believed to be the foundation of the devastating world wars of the 20th century (Archer et al., 2002).

In the 21st century, the role of information technology and politics in warfare has been higher than ever (Chifu & Simons, 2023). Chifu and Simons (2023) also note that the development of technology has, for example, led to the widespread use of remote killing, not only on defined battlefields but also in private homes, with the use of drone warfare. The use of stone tools and rudimentary weapons in the Stone Age conflicts has now become a relic of prehistory. The Greek hoplite warfare, medieval armored cavalry, and early modern European warfare characterized by the use of gunpowder and cannons have all been antiquated. The development of weapon systems powered by technological innovations is so rapid that the 20th-century nuclear weapons are now almost overshadowed by the emerging prominence of cyber warfare. Computers and automated systems are considered the new frontier of modern conflict (Sartor & Omicini, 2016).

Modern warfare is evolving towards unmanned or human-replacing weapon systems in the form of armed drones and other remote-controlled devices. They allow human beings to be physically absent from the battlefield (Heyns, 2016). For example, during the Obama Administration, the U.S. adopted a "Third Offset" strategy to use technology to counter opponents' strengths. This approach emphasized AI to help machines make quick decisions, manage data, assist soldiers with wearable tech, and improve coordination between manned and unmanned systems across all domains of warfare (Freedman, 2017). Regarding the possibilities of cyber warfare, the 1991 National Research Council of the United States had warned that, as America depended on computers, tomorrow's terrorists may be able to do more damage with a keyboard than with a bomb (Freedman, 2017).

The integration of AI into warfare presents profound ethical, strategic, and legal challenges. International Humanitarian Law (IHL), which governs the conduct of armed conflict, is struggling to keep pace with these rapid advancements. Core principles of IHL, which are distinction, proportionality, and humanity, face unique threats due to AI's inherent limitations, such as algorithmic bias, loss of human control, and challenges in accountability. For instance, autonomous systems risk violating the principle of distinction by misidentifying combatants and civilians, while cyber warfare complicates proportionality assessments and attribution of responsibility. Thus, the rapid advancements in AI and its integration with autonomous weapon systems (AWS) into warfare have outpaced traditional laws of armed conflict, necessitating a reevaluation of legal frameworks to address ethical, strategic, and humanitarian concerns.

Statement of the Problem

The increasing reliance on AI in modern warfare presents extreme challenges to existing IHL norms. Technologies like AWS may operate with minimal human intervention, raising concerns about accountability and compliance with the laws of armed conflict. Additionally, the use of AI in cyber operations complicates the attribution of responsibility and the assessment of proportionality, while AI-enhanced surveillance risks infringing on human rights. These developments expose gaps in current legal and ethical frameworks, necessitating a reexamination of IHL's ability to govern AI applications in warfare.

Thesis Statement

The rapid advancement of AI in armed conflict has outpaced the adaptability of IHL. This study argues that the deployment of AI-driven technologies, such as AWS and cyber warfare tools, poses significant risks to the foundational principles of IHL, which are distinction, proportionality, and humanity. The thesis asserts the urgent need for targeted legal frameworks to address these emerging complexities.

Objective of the Study

The objective of this study is to address the legal and ethical challenges posed by the integration of AI into armed conflict, specifically through the lens of IHL. By focusing on these challenges, it aims to contribute to the development of frameworks that reconcile technological advancements with humanitarian principles. For this, the study emphasizes the pressing need for international collaboration to evaluate existing laws, ensuring that IHL remains effective amidst these technological advancements.

Research Methodology

This study follows a qualitative research methodology to examine how laws governing armed conflict face challenges to address the AI integration into modern warfare. The research relies primarily on open-source data, particularly governmental and international organization reports and publications from recognized legal institutions. These primary sources are supplemented by a review of secondary sources, like journal articles, books, news articles, and other relevant publications. This paper applies descriptive and analytical approaches to study the ethical, legal, and practical effects of using AI in warfare. Under these approaches, the paper uses content, historical, and comparative analysis, along with relevant case studies. Relevant case studies are selected based on their significance in illustrating how AI technologies have been deployed in military operations and their legal and ethical implications. The criteria for selecting these case studies include their impact on IHL principles, representation of diverse geopolitical contexts, and the availability of verifiable data. This research is investigatory in nature, which aims to scrutinize the existing legal frameworks, identify gaps, and provide possible policy and legal suggestions for addressing the challenges of AI integration in armed conflict. These suggestions focus on the development of targeted legal and ethical frameworks that reconcile humanitarian principles with technological advancements. The scope of this paper is limited to examining the intersection of AI and IHL, particularly focusing on autonomous weapon systems, cyber operations, and AI-enhanced surveillance. While the study provides in-depth legal and ethical analysis, it does not encompass technical aspects of AI development or detailed national policies. Additionally, due to the reliance on open-source data, the findings may be constrained by the availability and reliability of such sources.

Evolution of International Humanitarian Law

A popular Latin aphorism, *inter arma leges silent,* often attributed to Cicero, roughly translates to “in time of war the laws are silent” (Solis, 2010). However, Solis (2010) notes that, even though soft, flexible, and malleable, there was a presence of some forms of rules of war since men began to fight. The notion that war should have rules is an ancient one. Belligerents used to have private agreements and pacts to govern the conduct of warfare (Crawford & Pert, 2015).

The efforts of the development of modern bodies of laws, that is, IHL, developed after the initiative of Sir Henry Dunant and ICRC in the nineteenth century. Today, this branch of public international law is largely codified in the four Geneva Conventions of 1949 and the Additional Protocols of 1977. Additionally, it has been considered that, over the past few decades, a body of customary law has evolved to govern the conflicts (Sassòli, 2019).Customary law refers to legal principles that have developed through consistent state practice and are generally accepted as binding.

IHL, as a whole, is a set of laws developed to mitigate the human suffering caused by armed conflicts. The primary aim of IHL is to limit the warfare and protect those who do not or no longer take part in the hostilities. It needs to balance this aim with another objective that is to protect the interest of the armed forces to prosecute the armed conflict (Crawford & Pert, 2015). The rise of AI and AWS is supposed to reshape warfare in the same way mechanization did in the 20th century.

Some general uses of AI in logistics and surveillance are widely accepted, but weaponized AI raises ethical and legal questions. Although militaries throughout the world are already using automated weapons, the targeting decisions are still largely controlled by humans (Heyns, 2016). However, some nations seem to be moving towards full autonomy without a 'man-in-the-loop,' meaning that AI systems independently make critical decisions in warfare without direct human intervention (Boothby, 2013). This is derived from Russian military commanders and U.S. defense officials hinting at the future of independent robots and fully autonomous weapons (Scharre, 2018). Therefore, the need to IHL today is to apply the general principles of IHL in the scenario of developed means and methods. This complicated development may explain why Hersch Lauterpacht (1952) once wrote that 'if international law is, in some ways, at the vanishing point of law, the law of war is, perhaps even more conspicuously, at the vanishing point of international law.'

Challenges of Autonomous Weapon System (AWS)

AWS poses significant ethical, legal, and operational challenges, particularly in their ability to comply with IHL principles. AWS is a system of robotic weapons that does not need human intervention once activated. They can select and hit the targets on their own. The presence of sensors, computers, and effectors arms them with situational awareness, information processing, and decision implementation (Heyns, 2016). According to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal AWS, AWS "are not one or two types of weapons. Instead, they are a capability category, i.e., a weapon system incorporating autonomy in its critical functions, specifically in target selection and engagement" (Hellman, 2024).

In his book Army of None, Paul Scharre (2018) presents two scenarios: First, during the Cold War, a Soviet officer manually overruled an AI-triggered nuclear launch alert, preventing the end of the world. It was a decision a machine might not have made. Second, in Afghanistan, Scharre's sniper team faced a young girl as a Taliban scout in disguise. He concluded that a robot would not know it may be wrong and immoral to kill in certain circumstances even if it is lawful. In these contexts, Scharre (2018) highlights the challenges of AWS and the irreplaceable human capacity for context and moral consideration. Despite the challenges, robots today are transforming wars just like they are transforming other industries, such as self-driving cars and cleaners. Many countries are investing their defense budget in military robots (Scharre, 2018).

Global spending on military robotics was $13.4 billion in 2022, which is expected to reach $30 billion in 2032 (Global Market Insights, 2023). The U.S. Air Force's Unmanned Aircraft Systems Flight Plan (2009–2047) envisions a future where competition for faster-than-ever speed and automation in unmanned aircraft would be similar to automated stock trading (Scharre, 2018).

The growth of AWS brings challenges in the fundamental principles of IHL. The rules of distinction, proportionality, and precautions have been challenged more than anything, and this issue needs to be a priority (Heyns, 2016). The rule of distinction states that only legitimate targets should be attacked. It distinguishes between the military objects and civilian objects. However, in the above example given by Scharre, the young girl scouting for the Taliban was technically a legitimate target. But in the real world, the humane rules of distinction go beyond the mechanical distinction, and that produces a test for AWS (Saxon, 2013).

Similarly, the principle of proportionality provides that any incidental or collateral damage inflicted on civilians who are not directly participating in hostilities must not be excessive in relation to the military advantages obtained. And thirdly, the principle of precaution requires taking feasible precautions in order to protect civilians (Heyns, 2016).With the development of AWS, the application of these principles of IHL has become more critical than ever in an attempt to achieve an equitable balance between humanitarian requirements and the necessities of war (Saxon, 2013).

William Boothby (2013), in his analysis, distinguishes between remotely operated and autonomous unmanned aircraft. He notes that remote operations typically do not raise specific IHL issues in principles of distinction and proportionality. They apply similarly across conventional, remote, and autonomous systems. However, autonomous systems face challenges in complex assessments, such as proportionality.It is reported that the fully autonomous weapons have already been used in Ukraine and Gaza (Hellman, 2024).

The war in Ukraine has been one of the first armed conflicts to use the killer robots. Similarly, evidence shows that AI tools are actively used for target identification in Gaza, that contributes to indiscriminate strikes, significant civilian casualties, and allegedly violates international norms (Hellman, 2024). Analyzing these real-life situations, it is deemed that limited autonomous targeting could be feasible in remote, predictable areas, but human oversight is a must. The parties need to ensure reliable monitoring and override capabilities through advanced technologies in order to expand the safe use of autonomous attack systems (Boothby, 2013).

AI in Cyber Warfare

Cyber warfare refers to military activity that primarily makes use of computer systems and networks in order to attack those of the adversary (Woltag, 2011). AI has been deployed as a cyber weapon in actual reality for quite some time, even before the deployment of AWS (Taddeo & Floridi, 2018). The use of AI in cyber warfare is a distinct yet interconnected concept to AWS in modern warfare. They are different from each other in their operational domain. As discussed in the previous section, AWS are physical systems capable of executing real-world actions autonomously. However, cyber warfare affects digital spaces by manipulating or disrupting networks. They are interconnected, as both technologies depend heavily on complex, opaque software, which complicates attack attribution and accountability in IHL (Schmitt, 2020). Similar to AWS, cyber warfare presents new challenges in the IHL rules about distinction and proportionality (Saxon, 2013).

Cyber warfare does not always mean the involvement of AI. Way before the development of modern-day AI, there have been instances of cyberattacks as stipulated above. Similar to traditional battleground warfare, cyber warfare can be conducted manually as well. However, in modern days, cyber-relevant strategies become increasingly reliant on artificial intelligence and preset action items, such as computational speed in execution and a situational awareness that assesses contested cyberspace in real time (Kallberg & Cook, 2017).

In April 2007, one of the earliest and most notable cyberattacks took place in Estonia. It was a prolonged series of distributed denial of service (DDoS) attacks that brought the banking system, many government services, and much of the media to a halt (Dinniss, 2012). In 2010, a virus called the Stuxnet worm hit Iran's computer networks, including its nuclear facilities (Dinniss, 2012). The development of cyber technology and its usage in war led the United States Department of Defence to treat the virtual environment of cyberspace as a new domain of warfare, subject to offensive and defensive military operations (Saxon, 2013).

AI is transforming the cyber warfare landscape as it enables both highly responsive defenses and aggressive, automated offensive capabilities. Automated cyber defenses, widely deployed in personal, corporate, and military spheres, handle the scale and speed of cyber threats through continuous, adaptive processes like those in firewalls and virus detection systems. Offensively, AI systems can autonomously analyze defenders' actions in real time, creating dynamic responses that outpace traditional defenses. This adaptability is powered by vast datasets from global cyber activity, which fuel AI's learning processes, making AI-driven cyber attacks increasingly agile and difficult to counter (Hallaq et al., 2017).

The complexity of AI in cyberattacks is such that the traditional rules and strategies no longer work because there will be no specific battlegrounds or armed forces. Additionally, AI, combined with social media, has become a powerful tool for indirectly influencing and mobilizing civilians for military advantages. Automation processes, like botnets and hashtag manipulation, allow AI to reach targeted audiences quickly and effectively. This technology has already been used to shape public opinion during major political events like U.S. presidential elections and even in military contexts, such as the Russian annexation of Crimea. With huge amounts of data available in the public domain, these tools can achieve specific effects, amplifying reach and precision in ways that were traditionally difficult to achieve (Schellekens, 2021).

AI offers a critical advantage in both network security and penetration, making it an essential tool for gaining superiority in cyber operations (Veiga, 2018).The extensive use of cyberspace in covert international operations shows an accelerating AI arms race (Kilovaty, 2018). Similarly, the widespread accessibility of AI-based cyber-attack tools and research suggests that malicious AI software is now commonly used (Haney, 2010).

Nations are striving to gain dominance in the domain of cyber warfare. In this context, there have been few global efforts to align cyber warfare with IHL, such as the Tallinn Manual, its new version 2.0, and studies from various organizations like NATO (Nunes, 2022). However, the absence of any specific binding agreements and the varying interpretations of limited legal sources have created challenges.

AI's Role in Surveillance and Precision Targeting

The report of the U.S. National Security Commission on AI (2021) states that, "The ability of a machine to perceive, evaluate, and act more quickly and accurately than a human represents a competitive advantage in any field–civilian or military. AI technologies will be a source of enormous power for the companies and countries that harness them." AI has reshaped the landscape of modern warfare, particularly in surveillance and precision targeting.

The weapon systems that are enhanced by AI use algorithms to identify, track, and engage targets with extraordinary accuracy and speed. These systems incorporate extensive training datasets and can autonomously process sensor data, distinguish valid targets, and even conduct targeted strikes. For example, image recognition algorithms scan through vast video feeds to pinpoint enemy activity. Similarly, facial recognition tools can identify individuals ,which makes AI a vital asset in intelligence gathering and real-time surveillance on battlefields (Goldfarb & Lindsay, 2022).

However, the claimed precision brought by AI in targeting has raised concerns for compliance with the principles of distinction and proportionality under IHL. AI has both strengths and risks in surveillance and precision targeting. Akerson argues that Offensive Lethal Autonomous Robots (OLARs) are fundamentally incompatible with IHL for several reasons. Primarily, the principles of distinction and proportionality in IHL necessitate human judgment and discretion. These are the qualities that rely on subjective decision-making and ethical considerations, which are beyond mathematical or algorithmic precision.

Akerson (2013) asserts that OLARs lack the capacity for true human-like judgment. Therefore, they cannot fully adhere to IHL's requirements, rendering them inherently unlawful under current interpretations of the law.Miniaturized autonomous systems are getting advanced that present complex implications for warfare. The trend of smaller, more mobile devices equipped with sophisticated sensors, navigation, and target recognition has grown. This enables the possibility of both military and non-state actors, including the terrorist groups, to leverage AI technology. These actors may exploit "quick and dirty" autonomous methods for efficient targeting without the ethical considerations that normally govern state warfare (Amoroso et al., 2018).AI's inability to fully comprehend the complexities of battlefield ethics, such as assessing proportional responses, complicates the argument for its unrestricted use (Akerson, 2013).

On the other hand, supporters contend that AI can potentially reduce collateral damage by accurately engaging military objectives.They claim that swarms of robotic systems fused with AI machine-learning techniques may presage a powerful interplay of increased range, accuracy, mass, coordination, intelligence, and speed in a future conflict (Johnson, 2020).Recent combat examples show the speed and efficiency brought by AI-enabled systems into targeting. For instance, in the 2014 Ukrainian conflict, Russia's instant reconnaissance-to-attack response highlighted the decisive power of an integrated AI-based kill chain model. Russia reportedly achieved a detection-to-engagement time of just 3–4 minutes in later exercises that marked a shift in combat power dynamics (Layton, 2021). This way, AI can significantly reduce human response times and strengthen operational impacts by the use of cloud computing, networked sensors, and command systems.

There is a concept of "human-machine teaming," which demonstrates that AI is helpful in supplementing the human decision-making process (Goldfarb & Lindsay, 2022). This concept allows operators to delegate specific judgment-based tasks to AI systems, such as determining the hostile intent of individuals in a populated area. As such, these technologies might theoretically offer an ethical advantage by prioritizing accuracy and reducing civilian casualties in conflict zones (Asaro, 2012). Advocates also argue that certain AWS might legally protect civilians with the help of better targeting accuracy. This is beneficial for both strategic advantages and also the rights of the civilians (Knuckey, 2016). However, the implementation of these principles depends on the successful integration of AI systems that maintain IHL standards.

Countries like China are actively exploring AI to modernize command and control by enhancing decision-making speed and accuracy on the battlefield. China's People's Liberation Army (PLA) uses AI for predictive planning and data fusion, demonstrating an early shift toward AI-led warfare (Layton, 2021). In naval warfare, AI-enabled defenses are reframing traditional tactical doctrines. One instance is commanders prioritizing advanced defense measures in an AI-filled environment, which is a shift from "attack first" strategies to "defend effectively first" (Layton, 2021).

The role of AI is further illustrated in long-range targeting with advanced missile systems equipped with deep reinforcement learning algorithms. These systems enable near pixel-perfect accuracy, suggesting a future where precision attacks are delivered with unmatched accuracy across vast distances (Haney, 2010). On one hand, these developments introduce tactical efficiency, while on the other, they raise concerns about the risks of reduced human control. Such risks are inevitable if precision-guided systems are exploited by aggressive AI-enabled strategies, as seen in China's rapid development and export of armed AI drones (Haney, 2010). The reliability of these systems under real-world conditions still remains a significant concern.

AI primarily relies on pre-existing data, which involves the risk of miscalculation, especially in high-stakes or volatile environments. In such cases, minor deviations from the training context could lead to catastrophic errors (Goldfarb & Lindsay, 2022). Such a problem is amplified in nuclear or near-nuclear scenarios, where the cost of miscalculation is prohibitively high and training data are often simulated due to the rarity of such events (Layton, 2021).

In reality, AI's application across military initiatives showcases its transformative potential in warfare. For instance, China's "intelligentized" cruise missiles and the U.S. Navy's LOCUST project demonstrate inevitable improvements in autonomous high-precision weapons. The U.S. Defense Advanced Research Projects Agency's unmanned vessel program and U.S. Marine "warbot companies" further illustrate the role of AI in continuous tracking and distributed sensing (Goldfarb & Lindsay, 2022). Meanwhile, Russia's rapid-reaction model in Ukraine and the U.S. "Loyal Wingman" program highlight the tactical advantages of AI-assisted rapid targeting. However, these implementations increase the need for oversight in AI-driven decision-making (Goldfarb & Lindsay, 2022). Taken together, AI promises enhanced surveillance and precision in military applications, along with the need for careful regulation to ensure ethical deployment. It is necessary to balance the capacity of AI for precise targeting with the IHL mandate of essential human judgment.

AI and National Security

The integration of AI and AWS into national security frameworks has intensified debates surrounding cyber sovereignty, ethical implications, and the preservation of state sovereignty in an increasingly digital battlefield (Bächle & Bareis, 2022). In 2018, the U.K.'s Attorney General, Jeremy Wright, questioned whether there is a specific rule in international law prohibiting violations of territorial sovereignty through unauthorized cyber operations. The U.K. does not believe that any such specific rule exists for cyber sovereignty. Instead, it deems cyber operations as illegal only if they constitute an unlawful intervention or a use of force against another state as per the U.N. Charter. Opposingly, countries like France, the Netherlands, Austria, and NATO members, except the U.K., assert that cyber operations without consent can violate sovereignty (Schmitt, 2020).

The concept of cyber sovereignty remains debatable regarding the types of effects that count as violations. Physical damage or permanent loss of functionality generally qualifies as violations. There is also debate over whether interference with core governmental functions like disrupting elections or law enforcement counts as a sovereignty violation, even without territorial damage. All things considered, passive defense in cyber seems typically acceptable. Alternatively, active and offensive cyber measures can result in infringing on another state's sovereignty, particularly when they involve autonomous capabilities.

In the view of national security, AI algorithms are used in military systems that play a crucial role in conducting modern combat activities on the battlefield. Additionally, these are important in terms of ensuring the proper functioning and the security of the state and all citizens (Bistron & Piotrowski, 2021). As Sayler (2019) notes, some key features of AI have made it relevant in the arena of national security. First, AI can get integrated across various applications and improve the 'Internet of Things.' Second, AI's dual-use nature allows for both civilian and military applications. For example, image recognition software can identify harmless objects on social media or assist in detecting terrorist or belligerent activity through drone surveillance.

Thirdly, AI is a transparent entity, which means it is often embedded within other technologies, making it not immediately noticeable in everyday products. For example, the U.S. military might acquire AI software for analyzing drone footage. They do not need to purchase a separate physical device.Obtaining an algorithm to add to existing surveillance systems would be sufficient. This means that AI isn't a single, countable item, like a new vehicle. But it is rather an invisible part of larger systems that often blends into the background.

Global powers like the U.S., China, and Russia illustrate the growing role of AI in redefining national security and asserting dominance in geopolitical conflicts. All use AWS to assert national power, embedding it in their military doctrines as tools of political communication. AI-driven weaponry and cybersecurity advancements are central to the escalating arms race among them (Haney, 2020). The U.S. applies broad definitions of AWS, which is framing them as automated systems. It is supposed to maintain flexibility in deployment without regulatory limits. It prioritizes AI in defense to counter cyberattacks that occur daily, which emphasizes the shift toward a continuous, digital battlefield.

On the other hand, China presents AWS as a symbol of its emerging AI dominance, positioning itself as an assertive global power. It has developed AI-guided missile technology and other advanced systems. Both nations use AWS as 'geopolitical signifiers' to reflect their visions of global order and project military strength and national pride (Bachle & Bareis, 2022). Meanwhile, Russia has leveraged AI in cybersecurity for tactics like social media manipulation to influence international political events (Haney, 2020).

Interestingly, some claim that the expansion of AI in military systems has posed challenges to state sovereignty as it enables non-state actors to exercise power and influence in ways that were previously not possible. (Usman et al., 2023). In parallel, the integration of

AI has also enhanced the surveillance capacities of the states to strengthen their protection over their populations, which consequently reinforces their national security. These countries are pursuing powerful AI systems to assert dominance, making national security dependent on these rapidly developing technologies.

Conclusion and Recommendations

The growing use of AI in armed conflict represents a revolutionary shift in the landscape of modern warfare. It confers operational advantages, including precision and speed, but further raises exclusionary in-depth ethical and legal challenges to IHL. While AWS and AI-powered weapons are not explicitly prohibited, their deployment must still respect the fundamental principles of IHL, including distinction and proportionality. The existing legal framework under the Geneva Conventions requires a distinction between combatants and civilians and prohibits attacks that are indiscriminate or disproportionate. It also requires states to assess every new weapon for compatibility with IHL. But existing mechanisms are not enough to scrutinize AI's autonomous decision-making. It is necessary to create legal regimes that are specifically tailored for the risks of AI and AWS. A regulatory response may take the form of a new protocol under the Geneva Conventions, amendments to the UN Convention on Certain Conventional Weapons (CCW), or the establishment of a separate treaty. The International Court of Justice could also issue an advisory opinion addressing state responsibility for AI warfare.

The remaining unsolved legal dilemmas are accountability and attribution. International criminal law focuses on individual responsibility, which is inadequate for AI-infused warfare. Existing frameworks do not provide for how liability should be assigned when autonomous systems operate outside of human intent or control. The legal arena needs new accountability mechanisms to close these gaps, such as state responsibility frameworks or specialized AI war crimes tribunals. But accountability alone will not be enough. Even legally attributable actions would fall outside IHL's ethical bounds if they lack meaningful human control. In this context, autonomous targeting (where direct human oversight is absent) poses an especially grave risk of unintended escalation, of misidentification of combatants, and of systemic violations of IHL. Meaningful human control safeguards need to be upheld to remain with the principles of necessity and humanity.

Legal compliance is still just a small part of the challenge.The unregulated proliferation of AI-driven weapons technology poses immediate and nearby existential threats to the sovereignty of the nation-state, and to global stability. The use of artificial intelligence capabilities in cyber warfare, automated retaliation systems, and asymmetric conflicts offers states and non-state actors new and unprecedented advantages in many different arenas.In light of these challenges, it is crucial that the international community move quickly. It is urgent for states, international organizations, and legal experts to work together to formulate binding legal norms. Such norms must ensure that systems utilizing AI in warfare comply with IHL principles and state responsibility in order to guarantee global stability. Without decisive intervention, unchecked militarization of AI will corrode the foundational pillars of IHL, undermine legal accountability in warfare, and set dangerous precedents for future conflicts, destabilizing global security.

References

ABP News Bureau. (2024, October 10). *Nobel Prize In Literature: Here's What Internet Thinks Who Should Be Winner In 2024 – Answer Will Leave You In Splits*. ABP Live. https://news.abplive.com/trending/nobel-prize-literature-2024-internet-predictions-winner-opinions-1723397

Akerson, D. (2013). The illegality of offensive lethal autonomy. In D. Saxon (Ed.), *International Humanitarian Law and the Changing Technology of War* (pp. 65-98). Martinus Nijhoff Publishers.

Amoroso, D., Sauer, F., Sharkey, N., Suchman, L., & Tamburrini, G. (2018). *Autonomy in weapon systems: The military application of artificial intelligence as a litmus test for Germany's new foreign and security policy*. Heinrich Böll Foundation.

Archer, C. I., Ferris, J. R., Herwig, H. H., & Travers, T. H. E. (2002). *World History of Warfare*. University of Nebraska Press.

Asaro, P. (2012). On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross*, *94*(886), 687–709.https://doi.org/10.1017/S1816383112000768

Bächle, T.C.,& Bareis, J. (2022). "Autonomous weapons" as a geopolitical signifier in a national power play: analysing AI imaginaries in Chinese and US military policies.*European Journal of Futures Research*, *10*(20), 1-18. https://doi.org/10.1186/s40309-022-00202-w

Bistron, M., &Piotrowski,Z. (2021). Artificial intelligence applications in military systems and their influence on sense of security of citizens. *Electronics, 10*(7), 1-19. https://doi.org/10.3390/electronics10070871

Boothby, B. (2013). How far will the law allow unmanned targeting to go?. In D. Saxon (Ed.), *International Humanitarian Law and the Changing Technology of War* (pp. 45-64). Martinus Nijhoff Publishers.

Chifu, I., & Simons, G. (2023). *Rethinking Warfare in the 21st Century: The Influence and Effects of the Politics, Information and Communication Mix*. Cambridge University Press.

Crawford, E., & Pert, A. (2015). *International Humanitarian Law*. Cambridge University Press.

Dinniss, H. H. (2012). *Cyber Warfare and the Laws of War*. Cambridge University Press.

Freedman, L. (2017). *The Future of War: A History*. Public Affairs.

Global Market Insights. (2023, October). *Military Robots Market*. https://www.gminsights.com/industry-analysis/military-robots-market

Goldfard, A., & Lindsay J. R. (2022). Prediction and judgment: Why artificial intelligence increases the importance of humans in war. *International Security*, *46*(3), 7-50. https://doi.org/10.1162/isec_a_00425

Hallaq, B., Somer, T., Osula, A. M., Ngo, K., & Mitchener-Nissen, T. (2017). Artificial intelligence within the military domain and cyber warfare. *Proceedings of 16th European Conference on Cyber Warfare and Security, Ireland(29-30 June)*.

Haney, B. S. (2020). Applied artificial intelligence in modern warfare and national security policy. *Hastings Science and Technology Law Journal*, *11*(1), 61-100. https://dx.doi.org/10.2139/ssrn.3454204

Hellman, J. (2024). The impact of autonomous weapons systems on armed conflicts: Are international humanitarian law norms offering an adequate response?. In D. H. Martínez & J. M. C. Cisneros (Eds.), *International Relations and Technological Revolution 4.0: World Order, Power and New International Society* (pp. 155-172). Springer.

Heyns, C. (2016). Autonomous weapons systems: living a dignified life and dying a dignifieddeath. In N. Bhuta, S. Beck, R. Giib, H. Y. Liu, & C. Kreb (Eds.), *Autonomous Weapons Systems: Law, Ethics, Policy*(pp. 3-19). Cambridge University Press.

Johnson, J. (2020). Artificial intelligence, drone swarming and escalation risks in future warfare. *The RUSI Journal*, *165*(2), 26-36. https://doi.org/10.1080/03071847.2020.1752026

Kallberg, J., & Cook, T. S. (2017). The unfitness of traditional military thinking in cyber. *IEEE*, *5*, 8126-8130.https://doi.org/10.1109/ACCESS.2017.2693260

Kilovaty, I. (2018). Doxfare: Politically motivated leaks and the future of the norm on non-intervention in the era of weaponized information. *Harvard National Security Journal*, *9*, 146-179. https://ssrn.com/abstract=2945128

Knuckey, S. (2016). Autonomous weapons systems and transparency: Towards an international dialogue. In N. BHUTA, S. BECK, R. GEIß, H. Y. LIU, & C. KREß (Eds.), *AutonomousWeapons Systems: Law, Ethics, Policy* (pp. 164-184). Cambridge University Press.

Lauterpacht, H. (1952). The problem of the revision of the law of war. *British Yearbook of International Law, 29*, 360-382.

Layton, P. (2021). *Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars*. Australian government department of defense, joint studies paper series No. 4.

Mollick, E. (2024). *Co-Intelligence: Living and Working with AI*. Portfolio | Penguin.

National Security Commission on Artificial Intelligence. (2021). *Final Report.*https://www.nscai.gov/wp-content/uploads/2021/03/Full- Report-Digital-1.pdf

Nunes, A. S. (2022). *The Legality and Accountability of Autonomous Weapon Systems: A Humanitarian Law Perspective*. Cambridge University Press.

Russell, S., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach* (3rd ed.). Pearson.

Sartor, G., & Omicini, A. (2016). The autonomy of technological systems andresponsibilities for their use. In N. BHUTA, S. BECK, R. GEIß, H. Y. LIU, & C. KREß (Eds.), *Autonomous Weapons Systems: Law, Ethics, Policy*(pp. 39-74). Cambridge University Press.

Sassòli, M. (2019). *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*. Edward Elgar Publishing Limited.

Saxon, D. (2013). International Humanitarian Law and the Changing Technology of War. In D. Saxon (Ed.), *International Humanitarian Law and the Changing Technology of War* (pp. 1-16). Martinus Nijhoff Publishers.

Sayler K. M. (2019). *Artificial Intelligence and National Security*. Congressional research service. https://www.everycrsreport.com/files/20191121_R45178_ddbcce24a6fbf02ad9e81387b5623295ac60f017.pdf

Scharre, P. (2018). *Army of None: Autonomous Weapons andthe Future of War.* W. W. Norton & Company.

Schellekens, J. (2021). Release the bots of war: social media and Artificial Intelligence as international cyber attack. *Przeglądeuropejski*, *2021*(4), 163-179. https://doi.org/10.31338/1641-2478pe.4.21.10

Schmitt, M. N. (2020). Autonomous cyber capabilities and the international law of sovereignty and intervention. *International Law Studies, 96*, 549-576. https://ssrn.com/abstract=3755530

Solis, G. D. (2010). *The Law of Armed Conflict: International Humanitarian Law in War.* Cambridge University Press.

Suleyman, M., & Bhaskar, M. (2023). *The Coming Wave: Technology, Power and the Twenty-First Century's Greatest Dilemma.* Crown.

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature, 556*, 296-298.https://doi.org/10.1038/d41586-018-04602-6

The Nobel Prize. (2024, October). *Nobel Prizes 2024*. The Royal Swedish Academy of Sciences. https://www.nobelprize.org/all-nobel-prizes-2024/

Usman, H., Nawaz, B., & Naseer, S. (2023). The future of state sovereignty in the age of artificial intelligence. *Journal of Law & Social Studies, 5*(2), 142-152.

Veiga, A.P. (2018). Applications of artificial intelligence to network security. *arXiv*,arXiv:1803.09992.

Warwick, K. (2012). *Artificial Intelligence: the basics*. Routledge.

Woltag, J. C. (2015). Cyber Warfare. *Max Planck Encyclopedia of Public International Law.* https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e280

-◆◆◆-