

ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 05 No. 01. Jan-March 2026.Page#.8564-8580
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

Autonomous Weapons and Algorithmic Warfare: Transforming National Security Paradigms in the 21st Century

Muhammad Haroon
Lecturer, Pakistan Studies, Department of Pakistan Studies, Kohat University of Science and Technology, KP
mharoonkp94@gmail.com
Abdur Rehman
Lecturer, Department of Political Science, University of Lakki Marwat.
rehmanmarwat118@gmail.com
Sumaira Gul
Lecturer, Political Science, Department of Political Science, Kohat University of Science and Technology, KP.
sumairagul526@gmail.com
Correspondence Author*: mharoonkp94@gmail.com

Abstract
This paper explores how Autonomous Weapons Systems (AWS) and Algorithmic Warfare are changing traditional ideas of national security. Traditional security thinking has mainly focused on human decision-making, state actions for which responsibility can be clearly established, and escalation processes that develop relatively slowly. However, the increasing use of artificial intelligence in military operations is challenging these traditional assumptions. The study uses a qualitative, document-based research approach and examines official defence policies, United Nations records, recent peer-reviewed academic studies, and investigative reports. Study focuses on five contemporary cases: i) the Russia-Ukraine war, ii) Israel's use of AI-assisted targeting in Gaza, iii) the United States' Replicator-to-Defense autonomous Warfare Group (DAWG) programme, iv) China's doctrine of "intelligentized warfare," and v) the India-Pakistan crisis of May 2025, known as "Operation Sindoor." The research study also presents a five-level classification of algorithmic threats, ranging from systems that support human decisions under human supervision to fully autonomous swarming and cognitive warfare. In addition, it compares how the United States, the European Union, the United Nations, and China are responding to the challenges of governing military AI. The findings suggest that algorithmic warfare can shorten decision-making time, make it more difficult to distinguish between offensive and defensive actions, weaken legal accountability, and increase security tensions between nuclear-armed rivals such as India and Pakistan. The paper concludes by recommending stronger national and regional frameworks for governing military AI. It particularly emphasizes the need for South Asian countries to develop a clear doctrine and establish confidence-

building measures to prevent the rapid escalation of algorithmic warfare from moving beyond political control.

Keywords: *Autonomous weapons, algorithmic warfare, artificial intelligence, national security, lethal autonomous weapons systems, strategic stability, South Asia.*

Introduction

National security refers to a state's ability to protect its sovereignty, territorial integrity, population, and vital interests from internal and external threats. Traditionally, national security relied on human control over the use of force, the ability to identify the source of an attack, and sufficient time for political leaders to manage military crises. However, artificial intelligence (AI), autonomous weapons systems, and algorithmic warfare are challenging these assumptions by changing how military decisions are made and how quickly operations can be conducted.

Artificial intelligence enables computers to analyse information, identify patterns, and support decision-making. Autonomous weapons systems (AWS) can select and engage targets without further human intervention once activated, while algorithmic warfare involves the use of computational algorithms in intelligence analysis, target identification, threat assessment, and military operations. Although these technologies improve the speed and efficiency of military activities, they raise concerns about human control, targeting accuracy, and accountability for the consequences of armed conflict. These changes reflect the broader revolution in military affairs, driven by precision-guided weapons, advanced surveillance, and interconnected military systems. The more recent concept of intelligentized warfare, particularly associated with Chinese military modernisation, highlights the growing role of AI, data processing, and intelligent technologies in military operations. As a result, military decisions may be made more quickly, leaving less time for human judgment and political intervention.

These technologies are becoming increasingly significant in recent times with the recent wars. Drones and unmanned aerial systems have been a key component of frontline operations in Ukraine and have been linked to significant casualties on the battlefield (U.S. Army War College War Room, 2025). In Gaza, allegations have been made regarding Israel's "Lavender" and "The Gospel" systems, which have led to worries regarding automatic target identification, target prioritisation, and the level of human review in terms of targeting decisions (Abraham, 2024). All these milestones mark the ethical and legal dilemmas of technology-enabled militaries. These concerns are more salient in South Asia, where India and Pakistan are nuclear powers and have a history of military confrontation. The use of advanced military technologies such as drones, India's air-defence systems, and loitering munitions was brought to the forefront of the public and policy debate by the May 2025 crisis, which was widely referenced as "Operation Sindoor" (South Asian Voices, 2026; Indian Aerospace and Defence Bulletin, 2025). Under incomplete information and unclear adversarial intentions, decision makers may come under greater pressure if they can detect and target threats more quickly. But the specific applications of AI-based systems in this crisis will need to be verified from trustworthy sources.

The increasing significance of military AI also raises five core questions in the field of national security: deterrence, attribution, proportionality, human accountability, and the strategic implications of military AI. The purpose of deterrence is to cause the expected costs of an action to exceed the benefits of that

action. Under international humanitarian law, the principle of proportionality suggests that the proportion of expected incidental civilian harm to the expected concrete and direct military advantage must not be out of balance; the principle of attribution is to identify who is responsible for an attack. The issue of human accountability relates to who is accountable for decisions on the use of force, including individuals and institutions. Automated responses can limit crisis management, complex technologies can make it harder to determine who is attacking, and inaccurate information can impact targeting decisions. In the same way, it may be more challenging to establish liability for illegal or incorrect attacks in cases where military forces and systems are engaged in an attack.

These challenges have clear links with the security dilemma and strategic stability of South Asia. The security dilemma is a situation in which a state's actions taken to enhance its security are viewed as a threat by another state, leading to a response that increases insecurity for both states. Strategic stability is when states have few reasons to start a conflict or launch a first strike and feel confident that crises won't quickly turn into a major war. By altering perceptions of military advantage, minimizing decision making time, and making it harder to determine an opponent's intentions and capabilities, autonomous weapons, AI-powered surveillance, and quicker targeting systems could impact both of those factors.

Literature Review

Ali and Zou (2026) explain that research on military artificial intelligence has expanded considerably in recent years. Earlier discussions, including the influential work of Paul Scharre, established an important foundation for understanding the different levels of human involvement in autonomous weapons. These levels range from systems in which humans remain directly involved in decisions to use force to fully autonomous weapons, often described in public debates as “killer robots”. Building on this foundation, existing scholarship has developed along three main lines: legal and ethical concerns, the practical military use of AI technologies, and their implications for regional security. Together, these areas provide a basis for examining how autonomous weapons are changing the traditional understanding of warfare and national security.

Digital Watch Observatory (2026) and the United Nations Office for Disarmament Affairs (2026) discuss the legal and ethical questions surrounding autonomous weapons systems, particularly their compatibility with international humanitarian law. This area of research mainly examines two important legal principles: distinction and proportionality. The principle of distinction requires parties to an armed conflict to differentiate between civilians and combatants, while proportionality prohibits attacks in which the expected incidental civilian harm would be excessive in relation to the concrete and direct military advantage anticipated. These requirements have raised concerns about whether autonomous systems can reliably assess complex battlefield situations and make appropriate targeting decisions. International discussions on these issues have continued through the United Nations Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE on LAWS), established under the Convention on Certain Conventional Weapons framework. Despite years of deliberations since 2016, these discussions had not produced a legally binding instrument by the time reflected in the cited sources. This continuing debate demonstrates the difficulty of developing international rules that address technological developments while maintaining effective human control over the use of force

Defense One (2026) and the Congressional Research Service (2026) examine the growing integration of AI-enabled technologies into military planning, procurement, and operational activities. Their work highlights the United States' Replicator Initiative and subsequent developments associated with the Defense Autonomous Warfare Group (DAWG). These initiatives illustrate the increasing emphasis on developing and deploying autonomous and semi-autonomous systems at scale. This literature helps explain how AI is becoming part of long-term defence planning rather than remaining confined to research laboratories or small-scale pilot programmes. It also raises questions about military preparedness, the speed of technological competition, and the implications of large-scale autonomous weapons deployment for international security.

Abraham (2024) and Artificial Weapons (2026) investigate the Israeli military use of AI-assisted targeting technology in Gaza. In their conversations they talk about systems that are said to be used to identify, assess and prioritise potential targets, such as “Lavender” and “The Gospel.” This research work has raised awareness of the degree of human involvement in setting targets and the dangers of using computer-based assessments in an armed conflict. Other questions in the literature could be raised regarding the accuracy of targeting information, civilian protection, and decision-making responsibility in relation to automated systems. Indeed, such developments are relevant to discussions on international humanitarian law, as the law does not abate its duties in relation to the conduct of hostilities due to the efficiency of technology.

Foreign Policy Research Institute (2025) and RAND (2026) examine the concept of intelligentized warfare of China, often referred to as the Chinese term zhihuihua. This method emphasises the role of artificial intelligence and data analysis, information integration and the application of advanced technology in military operations. According to the relevant literature, China is interested in these capabilities to facilitate more efficient and effective joint operations, efficiency, and decision-making within the armed forces. It also takes into account the importance of information and cognitive-domain operations, which aim to shape the opponent's interpretation of information, threat evaluation, and decision-making. This view extends the debate beyond the horizon of autonomous weapons and demonstrates the consequences of AI on strategic competition in other aspects such as surveillance, information management, and military planning. But the scope and utility of these capabilities need to be carefully evaluated, and not just based on "strategic statements" but based on reliable evidence.

Irregular Warfare Initiative (2026), Defence Horizon Journal (2025), and South Asian Voices (2026), the military and strategic implications of the May 2025 crisis between India and Pakistan were discussed; their analyses underscore the key role played by drones, loitering munitions, and AI-driven air-defence systems in the confrontation. The crisis has therefore been given the significance of an important event in the evolution of the use of sophisticated military technology in the South Asian region. The findings of these studies contribute to the debate on the effectiveness of the current defence arrangements, the increasing significance of unmanned systems and the potential impact of increased speed in military operations on escalation control. They also highlight the need to separate out “AI-assisted” weapons from weapons that are fully autonomous, as advanced technology does not equate to autonomous weapons making final decisions to use lethal force. To understand the real implications of these

technologies for regional security, there needs to be a measure of how much human involvement is needed.

Theoretical Framework

This research paper uses two related theoretical approaches to explain the growing role of artificial intelligence (AI) in military competition between India and Pakistan. The first is the security dilemma, which occurs when one state develops new military capabilities for its own defence, but the rival state views these developments as a potential threat. In response, the rival also strengthens its military capabilities, creating a cycle of mistrust and insecurity. This situation is becoming increasingly important in South Asia, where recent research on AI-based military technologies suggests that autonomous systems may reduce the time available for decision-making between India and Pakistan (Ali & Zou, 2026).

The second approach is the Observe-Orient-Decide-Act (OODA) loop, a decision-making model originally developed for air combat. It explains how military advantage can depend on how quickly a state observes a situation, understands it, decides, and acts. In modern warfare, artificial intelligence can speed up this process, allowing one side to respond more quickly than its opponent. This ability to make faster decisions may provide a significant strategic advantage (South Asian Voices, 2026).

Together, these two approaches show that AI is not simply another addition to existing military technology. It may also change the speed, nature, and psychological aspects of security competition between India and Pakistan. As military decisions become increasingly automated and rapid, both countries may feel greater pressure to respond immediately to perceived threats. Consequently, the time available for careful consideration, communication, and diplomatic intervention may become shorter, increasing the risk of misunderstanding, unintended escalation, and conflict.

Research Methodology

The research method used in this study is qualitative and document-based, and the analysis technique is thematic case-study analysis to analyze the selected issues. The main sources are the U.S. Department of Defense Directive 3000.09 (2023), the European Union AI Act and documents from the United Nations Convention on Certain Conventional Weapons (CCW) and its Group of Governmental Experts (GGE). Secondary sources include peer-reviewed journal articles, reports from established research organizations and think tanks, such as Research and Development (RAND), the International Institute for Strategic Studies (ISS), the Congressional Research Service (CRS), and investigative journalism from +972 Magazine, Local Call, and defence-related publications like Defence One, Responsible Statecraft, and South Asian Voices.

The sources were selected based on their purpose to cover four critical contemporary security and military issues: Ukraine, Gaza, U.S.-China great power competition, and South Asia. Where practicable, specific statistics and claims are double-checked against at least two independent sources to ensure reliability of the findings. The material used in the study is not classified or restricted information. Rather, it relies on public documents, research, reports and media to provide transparency and for readers to verify the evidence on which the analysis is based.

From Human-Centric to Machine-Mediated Warfare: A Conceptual Shift

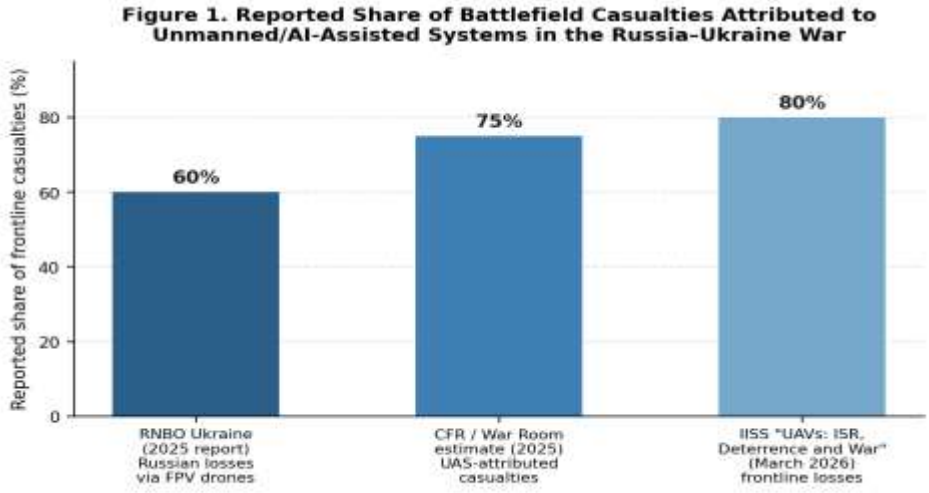
Traditional National Security Paradigms are built around an assumption, which could be called the human-decision assumption, that states a person in a chain of command and under the law in his/her home and international community grants permission to use deadly force. This is undermined by algorithmic warfare in two ways. It introduces decision-support systems that influence the human commander's view and their speed of decision-making, which pre-structures the decision where a human is formally "in the loop". Second, it brings in systems that are able to look for, select and engage targets without further human confirmation once they are activated, playing a role from decision-maker to system-designer and system-supervisor. Both of these shorten the OODA loop and shorten the time for political judgment, which is the very thing that most theories of deterrence and crisis management presume is plentiful.

Global Evidence and Case Studies

The Russia-Ukraine War: Attrition by Algorithm

Ukraine entered the war in February 2022 with fewer than one hundred drones in its inventory; by 2025 its industry had scaled toward an annual production target running into the millions of first-person-view (FPV) units, with more than 160 companies now manufacturing unmanned systems domestically (National Security and Defense Council of Ukraine, 2025). Unmanned aerial systems are now reported to account for the majority of frontline casualties on both sides, with the Ukrainian National Security and Defense Council citing FPV drones for roughly 60% of Russian losses (2025), the U.S. Army War College's War Room citing a 70-80 %range (2025), and the International Institute for Strategic Studies, in a March 2026 report, citing up to 80 % (Inkorr, 2026). A 2025 analysis by the Center for Strategic and International Studies found that removing the human radio-frequency link and replacing it with autonomous terminal guidance raised drone engagement success rates from roughly 10-20%to 70-80 %, precisely because autonomy removes the vulnerability created by jammable communications links (as cited in Resilience Media, 2026). Figure 1 summarises these independently reported estimates.

Figure 1



Note. Compiled by the author from National Security and Defense Council of Ukraine (2025), U.S. Army War College War Room (2025), and IISS estimates as cited in Inkorr (2026).

Importantly, Ukrainian officials have also acknowledged that fully autonomous drone swarms are unlikely to become a practical reality soon. They point to several ongoing challenges, including electronic warfare, dependence on weather conditions, and the low success rate of systems that rely entirely on manual control (Inkorr, 2026). This indicates that Ukraine's experience should not be viewed as a case of complete machine autonomy. Instead, it reflects a gradual but rapid shift towards greater autonomy, particularly during the final stage of an attack, when drones are more vulnerable to electronic countermeasures. The selective use of autonomous functions helps drones continue their missions even when electronic interference disrupts conventional control systems (VGI-9, 2026).

Israel-Gaza: Lavender, the Gospel, and Machine-Paced Targeting

The use of AI for lethal targeting has become a major case study in Israel, where the military has been conducting an operation in Gaza. The Gaza operation by Israel's military forces is one of the biggest applications of lethal targeting by AI. According to interviews with six Israeli intelligence officers, the Israel Defense Forces (IDF) subjected people to the AI system called Lavender, which assigned them a score between 1 and 100 based on their suspected affiliation with militant groups, in a 2024 investigation by +972 Magazine and Local Call. Though claims that it was inaccurate, the system reportedly identified by 37,000 potential targets (Abraham, 2024).

The investigation also highlighted the other two systems: The Gospel, which identified the buildings for possible attack, and “Where's Daddy?”, which alerted operators when the target returned home, reportedly allowing attacks to take place while family members were present (Abraham, 2024). The IDF, however, disputed certain of these claims and insisted the systems helped human analysts make final decisions about the targets, but did not make any decisions on their own (Lieber Institute, 2024).

The case is deeply concerned with the lack of humanity in AI-powered warfare. But in terms of individual verification, where each target is closely scrutinized, the pace and scale of AI-driven targets have raised

questions among legal experts about the extent to which meaningful individual verification has been possible (Brill/Journal of International Humanitarian Legal Studies, 2025). this shows that meaningful control is not guaranteed when human involvement is present, especially if targets are produced quickly by the AI systems and cannot be properly assessed by analysts.

The United States: From Replicator to the Defense Autonomous Warfare Group

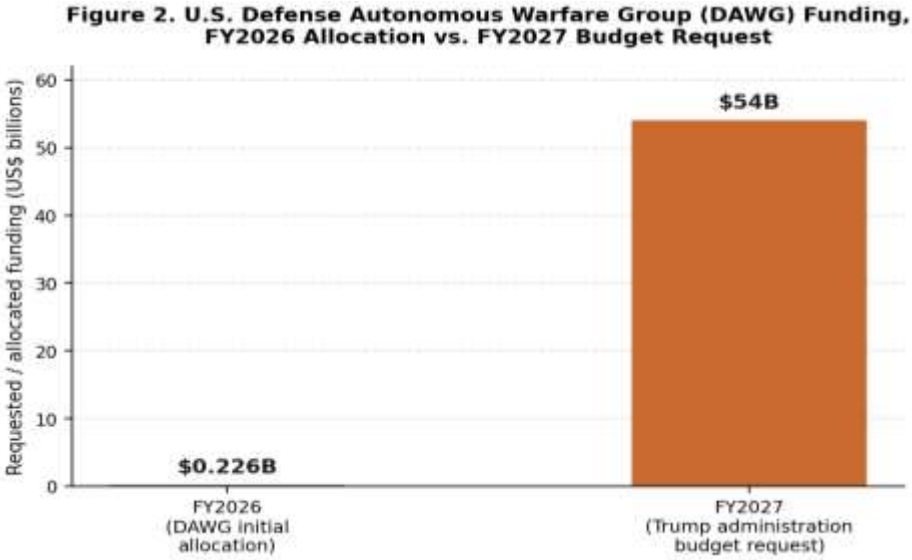
The United States provides another example of how quickly military institutions are moving towards autonomous warfare. In August 2023, then-Deputy Secretary of Defense Kathleen Hicks announced the Replicator Initiative. Its main objective was to deploy thousands of relatively inexpensive autonomous systems that could be replaced when lost or destroyed, within approximately two years. The initiative was designed partly to counter China's numerical advantage in military capabilities, particularly its large fleet of ships and extensive missile forces (Inkstick, 2025).

The initiative faced difficulties in meeting its original targets. By August 2025, the Congressional Research Service reported that only hundreds of systems, rather than the promised thousands, had been deployed. Continuing technical challenges and difficulties in the United States are another example of military institutions speeding up their autonomous warfare. The Replicator Initiative was announced by Deputy Secretary of Defense Kathleen Hicks in August 2023. It was designed primarily to deploy thousands of less costly, autonomous systems that could be replaced if lost or damaged, in about two years. It aimed in part to offset China's numerical superiority in military power, including its massive fleet of ships and vast missile forces (Inkstick, 2025).

But the project was beset with problems in achieving the original goals. As of August 2025, the Congressional Research Service said it had only seen dozens of systems as opposed to the promised thousands (Congressional Research Service, 2026). However, the acquisition process continued to face challenges and difficulties, further slowing its progress. The Pentagon officially retired the Replicator Initiative at the end of 2025 and handed its responsibilities to a newly created entity called the Defense Autonomous Warfare Group (DAWG) (Responsible Statecraft, 2025).

The change in organisation was not one of the U.S. backing down in its desire for autonomous warfare. Instead, further developments indicated a lot more institutional investment. DAWG's initial FY26 budget was about $225.9 million, and the FY27 budget is reported to be $54 billion. The huge jump indicates that autonomous warfare is no longer an experimental weapon and is now a more permanent part of U.S. military planning. The development could create the potential for "a permanent branch of the American military apparatus" of autonomous warfare, as Defense One wrote in 2026 (Defense One, 2026).

Figure 2



Note. Compiled by the author from Defense One (2026, May 22), "The Pentagon's $54 billion bet on autonomous warfare."

Parallel to DAWG, the U.S. Air Force's Collaborative Combat Aircraft (CCA) programme is developing AI-piloted "loyal wingman" drones intended to fly alongside crewed F-35, F-22, and B-21 aircraft, with autonomy software contracts awarded to Shield AI and RTX in December 2025 (Artificial Weapons, 2026). Legally, all of this activity is governed by DoD Directive 3000.09, updated in January 2023, which requires "appropriate levels of human judgment over the use of force" but does not define a precise threshold, does not prohibit lethal autonomy, and permits senior-level waivers of standard review procedures (Department of Defense, 2023; Human Rights Watch, 2023).

China: Intelligentized Warfare and Cognitive-Domain Operations

China's People's Liberation Army has made "intelligentization" a stated pillar of military modernisation since President Xi Jinping's 2017 call to accelerate the integration of AI into joint operations. Chinese military writing describes intelligentized warfare as extending beyond unmanned combat platforms into cognitive-domain operations, using large algorithmic models and generative AI to shape adversary perception and decision-making, an activity that PLA officers describe as potentially decisive "without even having to fight" a kinetic engagement (Defense One, 2025). China has also been reported to be developing a "counter-AI" doctrine that simultaneously deceives an adversary's data, algorithms, and computing power, including camouflage designed to fool machine-vision targeting and the deliberate injection of corrupted training data (Defense One, 2025).

South Asia: Operation Sindoor and the May 2025 India-Pakistan Crisis

In May 2025, India and Pakistan engaged in a four-day military confrontation involving aircraft, drones, and loitering munitions, known in Indian accounts as “Operation Sindoor” (South Asian Voices, 2026). India reported that its AI-based Akashteer air-defence system intercepted Pakistani drones and missiles, while open-source reports described the use of Harop, Warmate, and SkyStriker loitering

munitions against Pakistani military targets. The confrontation highlighted the growing role of artificial intelligence in speeding up military decision-making and improving battlefield responses.

Analysts suggest that India is increasingly moving towards deterrence by denial, while both countries continue to use autonomous systems mainly for tactical purposes. However, advances in autonomous drones may reduce dependence on vulnerable communication links and shorten decision-making time, increasing the risk of escalation between the two nuclear-armed states (Journal of Military and Strategic Studies, 2025; Irregular Warfare Initiative, 2026; Defence Horizon Journal, 2025).

Categorising the Threat Spectrum of Algorithmic Weapons

The case evidence above spans a wide range of human-machine relationships, from systems that merely advise a human operator to systems that independently plan and shape an adversary's perception of reality. To make this range analytically useful for policymakers, Table 1 organises algorithmic weapons into five threat tiers, moving from the most human-supervised to the least.

Table 1

A Five-Tier Taxonomy of Algorithmic Weapons Threats

Tier	Category	Description	Illustrative Example
I	Human-in-the-loop decision support	Algorithms process data and recommend targets or courses of action, but a human must authorise every use of force.	Early-generation Gospel target-recommendation system (Abraham, 2024)
II	Human-on-the-loop supervised autonomy	The system selects and can engage targets on its own, while a human can observe and override the action within a limited time window.	AI-cued air-defence networks such as Akashteer (South Asian Voices, 2026)
III	Human-out-of-loop lethal autonomy	Once activated, the weapon independently searches for, identifies, and engages a target without further human confirmation.	Loitering munitions with terminal AI homing (Congressional Research Service, 2022)
IV	Swarming and collective autonomy	Multiple autonomous units coordinate with one another, divide tasks, and adapt formation without centralised human control of each unit.	Replicator/DAWG attritable drone swarms (Defense One, 2026)
V	Algorithmic and cognitive warfare	AI is used not to fire weapons but to shape perception, decision-making, and the information environment of an adversary or population.	PLA cognitive-domain operations and generative disinformation (Foreign Policy Research Institute, 2025)

Note. Developed by the author based on the case evidence reviewed in Section 6 and the definitional categories used in DoD Directive 3000.09 (Department of Defense, 2023) and the CCW GGE on LAWS deliberations (United Nations Office)

This taxonomy clarifies an important point often lost in public debate: the most legally and ethically contested tier is not necessarily Tier III, where a machine's independent action is at least visible and attributable to a specific weapon, but Tier V, where algorithmic warfare operates below the threshold of an identifiable "attack" altogether, shaping political perception and decision-making in ways that existing national security frameworks, built around discrete, attributable acts of force, are simply not designed to detect or deter.

Global Governance and Policy Responses

Governance of military AI has developed unevenly across major powers and international institutions. Table 2 compares the four most consequential frameworks examined in this paper.

Table 2

Comparative Governance Frameworks for Autonomous Weapons

Actor / Instrument	Core Position	Legal Status	Human Oversight Standard
United States - DoD Directive 3000.09 (2023)	Permits autonomous and semi-autonomous weapons under internal senior review; does not ban lethal autonomy.	Binding internal DoD policy, not international law	"Appropriate levels of human judgment" (undefined threshold)
European Union - AI Act, Art. 2(3) & Recital 24 (2024)	Excludes systems used exclusively for military, defence, or national-security purposes from the Act's scope.	Binding EU regulation, but military AI carved out	None specified; governed instead by international humanitarian law
United Nations - CCW Group of Governmental Experts on LAWS	Negotiating a possible instrument since 2016; 2024–2026 mandate to finalise "elements" of a text.	Non-binding deliberative process; no treaty yet adopted	Contested; no consensus definition of "meaningful human control"
China - "Intelligentized Warfare" doctrine	Pursues AI-enabled unmanned systems and cognitive-domain operations as a central modernisation goal.	Doctrinal and organisational, not codified in public law	Not publicly specified

Note. Compiled by the author from Department of Defense (2023), Human Rights Watch (2023), Artificial Intelligence Act (2024) Article 2 and Recital 24, United Nations Office for Disarmament Affairs (2026), Digital Watch Observatory (2026), and Foreign Policy Research Institute (2025).

The comparison highlights a major gap in the governance of autonomous weapons and military artificial intelligence. The United States mainly relies on internal administrative directives to regulate autonomous weapons rather than specific legislation. Similarly, although the European Union has introduced one of the most comprehensive laws on artificial intelligence, its AI Act explicitly excludes military applications from its scope (Verfassungsblog, 2024). At the international level, the United Nations has made progress in discussions on autonomous weapons. After nine years of negotiations, the process has achieved significant agreement among states on several key issues (Artificial Intelligence Act, 2024). In 2025, a joint statement supported by 42 states called for negotiations on a legally binding international instrument. However, the process remains non-binding, and although a report is expected before the Seventh Review Conference of the Convention on Certain Conventional Weapons (CCW) in 2026, there is no guarantee that a treaty will be adopted (Stop Killer Robots, 2025). China, meanwhile, follows its military intelligentization strategy, which is largely guided by internal military planning and strategic documents rather than publicly available legislation. These differences reveal a common problem: no international framework currently requires all major developers of military AI to follow a shared definition of “meaningful human control.” As a result, decisions about the development and use of autonomous weapons remain largely under the control of individual states. This creates a serious governance challenge because the same countries competing to develop advanced military AI are also

responsible for regulating their own activities, with no universally binding rules to ensure consistent accountability and human oversight (United Nations Office for Disarmament Affairs, 2025).

Discussion: How Algorithmic Warfare Is Upending Traditional Security Paradigms

Deterrence and Strategic Stability

Classical deterrence theory assumes that an adversary has enough time to assess the possible costs and benefits of an action before making a decision. However, the development of algorithmic warfare is reducing the time available for such decisions. AI-assisted air-defence systems and loitering munitions can detect targets and carry out strikes within seconds. Such capabilities were reportedly evident during the South Asian crisis of May 2025. As a result, political leaders may have less time to consider their options before responding to a perceived threat. This creates a serious challenge for traditional deterrence theory, which assumes that there is sufficient time between a provocation and a military response for leaders to assess the situation and avoid unnecessary escalation (South Asian Voices, 2026). Consequently, regional stability may increasingly depend on which side can respond more quickly rather than on the ability of both sides to exercise restraint. This shift is particularly dangerous in South Asia, where both India and Pakistan possess nuclear weapons and a rapid military response could increase the risk of escalation (Ali & Zou, 2026).

Sovereignty, Attribution, and Escalation Thresholds

Traditional approaches to national security depend on the ability to identify the state responsible for an attack and determine an appropriate response according to the seriousness of the incident. However, autonomous weapons and drone swarms make this process more difficult. Low-cost and expendable systems can be used in attacks that leave limited evidence of direct state involvement. The party responsible may also deny its role or deliberately minimise the incident through diplomatic statements. These challenges were reflected in the deniable nature of the drone exchanges between India and Pakistan in 2025 (India-Pak Drone, CUAS Power in Focus, 2025).

At the same time, information warfare and disinformation campaigns can weaken an opponent's decision-making capacity, public confidence, and social unity without involving a clearly identifiable military attack. China's People's Liberation Army (PLA), for example, has pursued approaches that seek to influence an adversary's perceptions and decision-making processes (Defense One, 2025). Such activities create difficulties for traditional national security frameworks because their effects may develop gradually and remain below the threshold at which an incident is clearly recognised as an armed attack under international law. This makes it harder for governments to identify the nature of a threat, determine responsibility, and decide when a response is justified.

Accountability and International Humanitarian Law

International humanitarian law requires parties to an armed conflict to distinguish between military targets and civilians and to ensure that the expected civilian harm of an attack is not excessive in relation to the anticipated concrete and direct military advantage. These obligations require careful judgment and effective human oversight. However, the growing use of artificial intelligence in military operations raises important questions about who is responsible when an algorithm contributes to a decision that results in civilian casualties.

The situation in Gaza illustrates how the speed and scale of AI-assisted targeting can create serious challenges for these legal obligations. Even when a human officer formally approves an attack, the large number of targets generated by AI systems may leave insufficient time for a meaningful assessment of each target. In such circumstances, human approval may become a procedural step rather than a genuine exercise of judgment (Abraham, 2024). Existing policy frameworks, including U.S. Department of Defense Directive 3000.09, recognise the importance of appropriate human judgment in the use of autonomous weapons. However, the meaning and practical requirements of such judgment remain open to debate (Human Rights Watch, 2023). This uncertainty raises concerns about accountability, particularly when an autonomous system makes an error, identifies the wrong target, or contributes to an unlawful attack. Clearer standards are therefore needed to establish the responsibilities of military commanders, system operators, and other relevant decision-makers (Brill/Journal of International Humanitarian Legal Studies, 2025).

The Security Dilemma and the Autonomous Arms Race

The evidence discussed in this paper supports an important argument: when a major power invests in autonomous warfare, other states may feel compelled to develop similar capabilities, even if the original investment is presented as defensive. This behaviour reflects the traditional security dilemma, in which measures taken by one state to improve its security can make other states feel less secure (Inkstick, 2025).

The United States' shift from the Replicator initiative towards a reported $54 billion DAWG budget was presented as a response to China's ability to deploy military systems on a large scale (Defense One, 2026). Similarly, China has promoted its military intelligentization strategy as part of its broader effort to strengthen its military capabilities and compete with the United States over the coming decades (RAND, 2026).

A similar pattern may emerge in South Asia. India's investment in AI-enabled air-defence systems and loitering munitions could be viewed by Pakistan as a potential threat to its security. Islamabad may consequently seek to develop comparable capabilities or adopt alternative military measures to offset India's perceived advantage. Such responses could intensify regional competition and encourage both countries to invest further in autonomous weapons. The result would be a security dilemma unfolding at a much faster pace than traditional diplomatic efforts and arms-control arrangements can manage (Ali & Zou, 2026). Without effective communication and confidence-building measures, technological competition could increase mistrust and make future crises more difficult to control.

Implications for Pakistan and South Asia

The findings of this paper highlight three major implications for Pakistan’s national security. First, the May 2025 crisis demonstrated that drones and AI-assisted weapons have become an important part of South Asia’s security environment, making it necessary for Pakistan to include these technologies in its defence planning and crisis-management strategies (Irregular Warfare Initiative, 2026; Defence Horizon Journal, 2025). Second, the limited public information about Pakistan’s military AI policy creates uncertainty about its capabilities and intentions. Clearer policy statements could improve understanding without revealing sensitive military information (Journal of Military and Strategic Studies, 2025). Third, the absence of effective regional arrangements for managing autonomous weapons increases the risk

of miscalculation and rapid escalation. Therefore, India and Pakistan need stronger communication channels, mechanisms to investigate disputed drone incidents, and discussions on the responsible use of AI in warfare. Although these measures cannot resolve all bilateral tensions, they could reduce mistrust and help prevent future military crises.

Policy Recommendations

- Pakistan should issue a public policy statement explaining its position on autonomous weapons and the principles that guide their development, acquisition, and use. The policy could follow the transparency approach of the US Department of Defense Directive 3000.09 without necessarily adopting the same rules. This would help clarify Pakistan's intentions and reduce uncertainty about its military doctrine.
- Pakistan and India should explore informal diplomatic discussions, either through a bilateral track-two dialogue or a suitable regional platform linked to SAARC. These discussions should focus on preventing AI-driven decision-making from increasing the risk of accidental escalation during a crisis. The experience of the May 2025 crisis provides an important basis for examining how faster decision-making could affect stability between the two countries.
- Pakistani policymakers should participate actively in the United Nations Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts (GGE) process on Lethal Autonomous Weapons Systems (LAWS), particularly ahead of the 2026 report to the Seventh Review Conference. These discussions will influence the future international rules governing autonomous weapons. Pakistan should therefore contribute to shaping these rules rather than simply responding to decisions made by other states.
- Universities and research institutions in Pakistan should invest more effort in studying military AI and autonomous weapons. Departments of Pakistan Studies, International Relations, and Strategic Studies can play an important role in this area. At present, publicly available research on Pakistan's own position and capabilities remains limited compared with the information available on India, the United States, and China. More research would help policymakers make informed decisions and develop a clearer understanding of the security challenges associated with these technologies.
- Any future acquisition of autonomous or semi-autonomous weapons by Pakistan should be supported by clearly defined and publicly available standards for human supervision. These standards should explain the responsibilities of human operators and the level of control required over critical decisions involving the use of force. Such measures would strengthen accountability under international humanitarian law and improve Pakistan's credibility in future arms-control negotiations.

Conclusion

Autonomous weapons and algorithmic warfare are changing the nature of modern conflict and creating new challenges for national security, deterrence, and international law. For Pakistan, these developments are particularly significant because of its strategic rivalry with nuclear-armed India. The May 2025 crisis highlights the importance of preparing for the risks associated with AI-driven military decisions. Pakistan must develop a clear national policy, strengthen research, promote regional dialogue,

and actively participate in international efforts to regulate autonomous weapons. Above all, technological advancement must not come at the cost of human judgment and accountability. Pakistan's ability to manage these challenges will be essential to protecting its national interests, preventing unintended escalation, and maintaining strategic stability in South Asia.

References

Abraham, Y. (2024, April 3). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. +972 Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/

Ali, J., & Zou, X. (2026). AI security dilemma and militarisation in South Asia: Rethinking strategic stability in the age of autonomous warfare. SAGE Open. https://doi.org/10.1177/21582440261475709

Artificial Intelligence Act. (2024). Article 2: Scope. https://artificialintelligenceact.eu/article/2/

Artificial Intelligence Act. (2024). Recital 24. https://artificialintelligenceact.eu/recital/24/

ArtificialWeapons. (2026a). Israel's AI targeting ecosystem: Lavender, Gospel, and the machine-led war in Gaza. https://artificialweapons.com/case-studies/israel-ai-targeting-gaza

ArtificialWeapons. (2026b). Pentagon Replicator program 2026: Inside America's $1B+ drone swarm initiative. https://artificialweapons.com/articles/pentagon-replicator-program-2026

Brill / Journal of International Humanitarian Legal Studies. (2025). The use of 'Lavender' in Gaza and the law of targeting: AI-decision support systems and facial recognition technology. Journal of International Humanitarian Legal Studies, 16(2). https://brill.com/view/journals/ihls/16/2/article-p336_003.xml?language=en

Congressional Research Service. (2026, January 21). DOD Replicator initiative: Background and issues for Congress (IF12611). Library of Congress. https://www.congress.gov/crs-product/IF12611

Congressional Research Service. (n.d.). U.S. policy on lethal autonomous weapon systems (IF11150). Library of Congress. https://www.congress.gov/crs_external_products/IF/HTML/IF11150.web.html

Defence Horizon Journal. (2025, December 9). Future of drone warfare in South Asia. https://tdhj.org/blog/post/drone-warfare-south-asia/

Defense One. (2025, November 24). To China's war planners, AI is just another thing to deceive. https://www.defenseone.com/threats/2025/11/chinas-emerging-counter-ai-warfare-playbook/409757/

Defense One. (2026, May 22). The Pentagon's $54 billion bet on autonomous warfare. https://www.defenseone.com/ideas/2026/05/pentagons-54-billion-bet-autonomous-warfare/413735/

Department of Defense. (2023). DoD Directive 3000.09: Autonomy in weapon systems. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf

Digital Watch Observatory. (2026). GGE on lethal autonomous weapons systems. https://dig.watch/processes/gge-laws

Foreign Policy Research Institute. (2025, March 18). AI dependence and political blind spots undermine Beijing's war strategy. https://www.fpri.org/article/2025/03/ai-dependence-and-political-blind-spots-undermine-beijings-war-strategy/

Frontiers in Political Science. (2026). Emerging patterns in intelligentized warfare: Speed, consumption, and the transformation of military operations. https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2026.1837867/full

Garamone, J. (2023, January 25). DOD updates autonomy in weapons system directive. U.S. Department of Defense News. https://www.globalsecurity.org/military/library/news/2023/01/mil-230125-dodnews01.htm

Human Rights Watch. (2023, February 14). Review of the 2023 US policy on autonomy in weapons systems. https://www.hrw.org/news/2023/02/14/review-2023-us-policy-autonomy-weapons-systems

India-Pak Drone, CUAS Power in Focus. (2025, June 11). Raksha Anirveda. https://raksha-anirveda.com/changing-warfare-an-assessment-of-india-pakistan-drone-and-cuas-capabilities/

Indian Aerospace and Defence Bulletin. (2025, September 16). The geopolitics of autonomous weapons technology. https://www.iadb.in/2025/09/12/the-geopolitics-of-autonomous-weapons-technology/

Inkorr. (2026, April 22). Drones overtake artillery for the first time: Up to 80% of frontline casualties now caused by UAVs. https://inkorr.com/en/amp/droni-vperse-viperedili-artileriu-do-80-vtrat-na-fronti-pripadae-na-bpla-318915

Inkstick. (2025, September 5). Deep dive: Pentagon's Replicator Initiative raises questions. https://inkstickmedia.com/deep-dive-pentagons-replicator-initiative-raises-questions/

Irregular Warfare Initiative. (2026, July 11). The strategic use of drones in Pakistan-India irregular warfare. https://www.irregularwarfare.org/india-pakistan-drone-warfare/

Journal of Military and Strategic Studies. (2025). India's use of AI in the 2025 border conflict. https://jmss.org/article/download/81710/58756/274603

Lieber Institute. (2024, September 6). Israel-Hamas 2024 symposium: The Gospel, Lavender, and the law of armed conflict. West Point. https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/

Loitering Munitions and the Emergence of India's AI [enabled drone doctrine]. (2025). TIJER. https://tijer.org/tijer/papers/TIJER2511127.pdf

National Security and Defense Council of Ukraine. (2025). Results of Ukraine's defense industry in 2025: FPV drones. https://www.rnbo.gov.ua/en/Diialnist/7370.html

RAND Corporation. (2026, March 4). The People's Liberation Army's perspectives on artificial intelligence highlighting integration as key to "intelligentization" goals. https://www.rand.org/pubs/perspectives/PEA4574-1.html

Resilience Media. (2026, July 12). In the era of precise mass, FPVs are outgrowing the pilot. https://resiliencemedia.co/in-the-era-of-precise-mass-fpvs-are-outgrowing-the-pilot/

Responsible Statecraft. (2024, April 5). Israel using secret AI tech to target Palestinians. https://responsiblestatecraft.org/israel-ai-targeting/

Responsible Statecraft. (2025, November 1). DoD promised a 'swarm' of attack drones. We're still waiting. https://responsiblestatecraft.org/replicator/

South Asian Voices. (2026, January 1). Next generation air warfare in South Asia: Risks and way forward. https://southasianvoices.org/sec-m-pk-r-next-gen-air-warfare-in-south-asia-1-1-2026/

Stop Killer Robots. (2025, November 6). 156 states support UNGA resolution on autonomous weapons. https://www.stopkillerrobots.org/news/156-states-support-unga-resolution/

U.S. Army War College War Room. (2025, August 21). Artificial intelligence's growing role in modern warfare. https://warroom.armywarcollege.edu/articles/ais-growing-role/

United Nations Office for Disarmament Affairs. (2025, October 23). Briefing by the Chair of the CCW GGE on LAWS on the margins of the First Committee. https://disarmament.unoda.org/en/updates/briefing-chair-ccw-gge-laws-margins-first-committee

United Nations Office for Disarmament Affairs. (2026). Convention on Certain Conventional Weapons - Group of Governmental Experts on Lethal Autonomous Weapons Systems (2026). https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2026

VGI-9. (2026, March 11). From quantity to algorithms: How FPV warfare is changing in 2026. https://vgi.com.ua/en/from-quantity-to-algorithms-how-fpv-warfare-is-changing-in-2026/