MSI Journal of
Arts, Law and Justice (MSIJALJ)

Weaponized AI: The Rise of Robots and Drones in Modern Terrorism

Dr. S. Rajalakshmi[1*]

[1*]Associate Professor & Head, Department of Criminal Law and Criminal Justice Administration, The Tamil Nadu Dr. Ambedkar Law University.

*** Correspondence:** Dr. S. Rajalakshmi

The authors declare that no funding was received for this work.

OPEN ACCESS

Received: 29-March-2026
Accepted: 27-April-2026
Published: 02-May-2026

This article is published by **MSI Publishers** in **MSI Journal of Arts, Law and Justice (MSIJALJ)**
ISSN 3049-0839 (Online)

The journal is managed and published by MSI Publishers

Volume: 3, Issue: 5 (May-2026)

ABSTRACT: We are witnessing profound changes in warfare in the current era, particularly with the adoption of robots and drones. As instruments of conflict, they transform the social space where interlocutors interact with each other. The power imbalance between states and non-state actors has significantly diminished due to the fact that terrorists have rapidly integrated drone systems and robots into their operations. This has been made possible through the commercialization of warfare and the liberalization of weapons technology. Terrorist groups have adopted these techniques, leading to threats in several Middle Eastern and African countries. The use of drones has transformed counterterrorism strategies and tactics worldwide, raising serious ethical and legal concerns. Efforts have been made at the international level to regulate the transfer of drone technology, and countries are working to radically change their response strategies against terrorism. Their current objective is to develop defensive and preventive measures to combat terrorism.

Keywords: *Drones, Post-Human Wars, Drone Warfare, Anti-Drone Measures, Ethical Concerns.*

INTRODUCTION

Robotic drones and autonomous robots by the United States in Afghanistan, Iraq, and other regions has led to the

proliferation of drones among military forces and terrorist organizations. This technological expansion has extended across land, air, and sea, disrupting traditional military strategies and giving rise to new dynamics in warfare. Terms such as unconventional warfare, drone warfare, and hybrid warfare have emerged to describe the impact of modern technology on the nature of conflicts. Historically, issues of war and security were among the primary concerns of states in their struggle for supremacy, which was largely confined to inter-state relations. The arms race between the United States and the former Soviet Union serves as a notable example. Today, the integration of aircraft, drones, and robots in warfare is no longer limited to state actors. The increasing role of economic and corporate interests in conflicts has reshaped the nature of warfare, raising concerns about the future of security engineering. The monopoly on warfare is no longer the exclusive domain of government representatives, as reliance on human personnel has significantly decreased, giving rise to new social realities and a post-human phenomenon. As a consequence of these developments, terrorist organizations have adopted these technologies as preferred tools to instil fear among the masses and achieve their political objectives.

This study highlights how drones and robots impact the tactical approaches of terrorist organizations. It explores key questions such as: How do drones and robots become a preferred choice for terrorist groups? How are these technologies adopted as new tactics in terrorism? What are the ethical and legal responsibilities associated with their use? How do these weapons alter counterterrorism efforts? And what political choices are available for the future? The study follows an inductive analytical approach, drawing on in-depth knowledge of the subject and incorporating ethical considerations. Data collection relied on secondary sources, including research articles, reports, journals, and opinion pieces from both print and digital media.

Information on Drones and Robots

Hall emphasizes that the concept of social space involves recurring domains or patterns, where actors direct their actions toward one another. This concept, widely applied in diplomacy, remains equally relevant in the study of warfare. The author

argues that social spaces emerge when common systems and laws largely determine the actions and behaviors of actors. However, the advent of new technologies has reduced the role of human soldiers, suggesting that future wars could be fought between robots. This perspective extends to examining the impact and role of drones and robots in terrorism, as well as their use in counterterrorism strategies. Consequently, autonomous unmanned vehicles may significantly reduce human soldier participation in future conflicts. The United States and 43 other countries are actively developing robots and drones, leading to an arms race among nations. Private sector companies are also investing in this field, contributing to the widespread diffusion and availability of these technologies in various countries and among non-governmental groups.

Since 2003, the United States has deployed approximately 7,000 drones and 12,000 ground vehicles, using them as snipers and to destroy terrorist hideouts. The U.S. has employed drones on multiple occasions, particularly in Afghanistan, Iraq, Pakistan, and other regions worldwide. Several authors suggest that future American wars could involve hundreds of thousands of robots and drones. Between 2005 and 2007, the British government acquired "Taranis," a fully autonomous aircraft capable of penetrating enemy territory, gathering intelligence, dropping bombs, and engaging in self-defense. These aircraft are designed to reduce human dependency, as remote operators may face delays in receiving signals and preparing for subsequent attacks. The company General Motors installed the first robotic arm for industrial use in 1961. Since then, robotics industries have expanded worldwide. By 2017, the global industry had more than 8.4 million robots in operation.

The United States has deployed *Predator* and *Landmark* drones in Pakistan, Somalia, and Yemen as part of Operation Enduring Freedom. U.S. forces have used drones in approximately 30,000 missions. Philosopher Graham Harman describes this technological evolution as the "Hidden Empire," where satellites, anti-tank explosives, and Landmark aircraft redefine the battlefield, gradually replacing human armies with robots —a phenomenon he calls "robot war." Initially, drones such as *Global Hawk* and *Predator* were primarily designed for intelligence gathering and automation. However, new trends are shifting toward autonomous surveillance and

decision-making in lethal operations. The integration of intelligence, surveillance, and reconnaissance capabilities with precision-guided systems has transformed drones into powerful tools for surveillance and targeted strikes, making them a critical component of modern warfare. As drone and robot development becomes more accessible, concerns are growing that terrorist groups may adopt these technologies as part of modern combat tactics. This issue will be discussed in the next section.

Country efforts to develop and benefit from the technologies of drone manufacturing

The drone industry is rapidly expanding across major industrialized nations and developing countries, particularly in Asia, where a series of reforms aimed at strengthening the drone sector has already begun. Regulations in some countries provide a necessary legal framework for the commercialization and use of drones. These regulations cover various aspects, including drone certification, registration and operation, airspace restrictions, research and development, testing, training and licensing, as well as violations and sanctions. The expansion of regulated drone airspace has opened a significant portion of many countries' skies, creating a "green space" for drones to operate at altitudes of approximately 400 feet.

In 2015, the Pakistani army announced that it had eliminated three high-ranking terrorists using the country's first locally developed drone. Major General Asim Bajwa, spokesperson for Pakistan’s military public relations department, stated in a social media post: *The first Pakistani drone, model "Barak," struck a terrorist compound in Wadi Shawal*. It is worth noting that drone strikes targeting militant hideouts in Pakistan’s tribal areas began in 2004, but these early attacks were conducted using American drones. In the same context, India announced that security forces had killed three terrorists in the Aarey area of Baramulla district, Jammu and Kashmir. The operation involved continuous drone surveillance, which tracked the terrorists and bombed their hideouts in the forests to drive them out. Experts debate the feasibility and effectiveness of relying on such technologies for counterterrorism efforts within national borders. However, there is no longer any doubt about the increasing use of drone technology in modern warfare against militant organizations.

According to some media reports, there is a growing demand for drone-mounted cameras. They indicate that "thermal drone technology" was first used in Pakistan during an operation against a terrorist compound on June 5, 2023, in Matni, a suburb of Peshawar. This was the first successful operation using "thermal imaging drones" supplied to Pakistan's Counterterrorism Directorate in Khyber Pakhtunkhwa. During the operation, the terrorists' hideout at the Metni-Adizai border with the Khyber region was targeted. However, the operation was interrupted due to nightfall. With the help of modern drones, aerial surveillance of the compound continued throughout the night, allowing security forces to monitor any movement and take necessary action. Due to intense gunfire from the Pakistani armed forces, the terrorists were unable to change positions or effectively retaliate.

The thermal technology mentioned above is a modern vision system capable of clearly detecting the movement of living beings in complete darkness. This technology easily identifies hidden individuals based on body heat. Thanks to its capabilities, the leader of the banned organization was killed in this operation, while another was injured. However, some accomplices managed to escape by hiding in the bushes and using a rainwater drain. The main terrorist who was eliminated had been involved in attacks on customs officials and a Pakistani police station. He was a member of the banned group known as "Chin Taliban Pakistan." Pakistani security officials expressed their satisfaction with the success of the operation, with a prominent spokesperson stating:

"If it were not for drone cameras, aerial surveillance of this location would have been impossible. Most importantly, our forces completed the mission without sustaining a single injury."

This demonstrates the growing demand among nations for drone-integrated technologies. As a result, military officers and technicians are increasingly being trained to operate these advanced systems. Reports from various countries indicate that some police and security agencies have implemented budget austerity measures to allocate additional funds for acquiring drones equipped with such technologies. This ensures the continuity of counterterrorism operations while minimizing risks to army personnel and security forces, keeping them safe from injury, capture, or death.

The highest officials of a country like Pakistan, including the Prime Minister, the Minister of Information, and top military and security agency officials, are actively involved in equipping the anti-terrorism department with modern tools. They emphasize that an "intelligent" approach to counterterrorism—leveraging contemporary technologies—is the most effective strategy. In some countries, such as India, the drone certification system has been revamped, making it easier for drone manufacturers to obtain type certification. Additionally, a new drone import policy has been introduced, prohibiting the import of foreign drones while allowing the import of their components. In this context, it is common for national aeronautical regulatory bodies to collaborate with various ministries to promote drone applications. They implement initiatives aimed at expanding drone use in commercial logistics, agriculture, mining, mapping, and industrial inspection. The utility of drones has significantly evolved, with applications including vaccine delivery, oil pipeline and power transmission line inspections, anti-locust control operations, agricultural spraying, and land surveillance.

Several countries are now establishing specialized training schools for drone operations. These ongoing developments in drone technology and policy are expected to accelerate the widespread adoption of drones, potentially reshaping the manufacturing and distribution landscape. In the near future, personal drone ownership may become more common, fundamentally altering how drones are used across industries and daily life.

In certain countries where individuals enjoy a comfortable lifestyle and greater freedom in trade and commerce, drone sales have become a highly profitable venture. According to Arab media reports, citizens of the United Arab Emirates (UAE) can earn more than 30,000 dirhams through the sale of drones. Additionally, salaries in the technology sector, particularly in the field of drones, are reported to be highly lucrative. Drone operators in the UAE typically earn between 4,800 and 13,700 dirhams per month.

Pakistani media have highlighted the growing opportunity for selling drones to Gulf countries, emphasizing the significant rise in information technology exports. Reports suggest that drone engineers in Pakistan could earn between 22,000 and

25,000 dirhams if they successfully cater to high-net-worth clients in wealthier nations. Meanwhile, engineers and professionals with expertise in artificial intelligence may earn more than 25,000 dirhams, according to the Economic Research Institute. This suggests that income levels for Pakistani professionals in this field can be up to ten times higher than those of their counterparts in other industries with similar academic qualifications. Alex Laperov, CEO of MicroAvia, noted that several sectors in the UAE are harnessing the potential of drones. The drone industry in the country is estimated to be worth $1.1 billion. To support this growing market, a dedicated drone manufacturing and training center was launched in 2022, further solidifying the UAE's position as a hub for drone technology and innovation.

Upsurge in the use of technology in Terrorism: types of Drones and Robots used in Terrorism

Overview of drone technology and Robotics

Technological advancements have enabled terrorist organizations to refine and modernize their strategies for future attacks. The development of unmanned aerial vehicles (UAVs) capable of autonomous decision-making in surveillance and targeted assaults has significantly enhanced their capabilities. Additionally, the use of "land robots" for field operations—previously reported during the Iraq War by the United States—demonstrates how automation is becoming integral to modern conflict. Terrorist activities are primarily designed to instill fear and pressure civil governments into making political concessions. The availability of drones and robots capable of executing multiple attacks has provided these groups with a more effective means of achieving their objectives. Factors such as mass production, the increasing accessibility of drone and robotic technology, and lower operational costs make them attractive tools for terrorists.

Historically, most terrorist groups relied on easily obtainable weapons and equipment. Over the past 35 years, major attacks like the Oklahoma City bombing and the 9/11 attacks were carried out using legally purchased materials. In addition to acquiring weapons, these attacks required individuals willing to sacrifice their lives or risk capture. However, the integration of drones and robotic systems has reduced

the reliance on human operatives while simultaneously enhancing the ability to conduct multiple attacks with minimal manpower.

In recent years, the widespread use of drones has drawn significant attention, particularly during the Russo-Ukrainian war. No longer restricted to military applications, drones have increasingly been exploited by terrorist organizations for attacks, reconnaissance, and smuggling operations. Terrorist groups have targeted numerous strategic locations across the Middle East using drones, striking military bases, oil depots, and airports. This shift in tactics has forced governments worldwide to adapt their defense and counterterrorism strategies to address these evolving threats.

Comparison of Capabilities and Uses

Yaacoub et al. classify the uses of drones and robots into two broad categories:

1. **Beneficial Uses –** These include commercial, law enforcement, and military applications, such as intelligence gathering, reconnaissance, counter-insurgency operations, and anti-terrorism measures.
2. **Harmful Uses –** These involve their exploitation by criminals and terrorist organizations for destructive purposes.

Terrorist Use of Drones and Robots

Terrorists have adapted drones and robotic technology for a variety of malicious activities, including:

- **Biological, Chemical, Radiological, and Nuclear (CBRN) Attacks –** Drones can be used to disperse hazardous substances over populated areas.
- **Propaganda and Psychological Warfare –** They can be employed for online psychological attacks, live-streaming terror activities, or spreading extremist propaganda.
- **Armed Attacks –** Drones can be equipped with explosives, firearms, or missiles for targeted strikes.

- **Surveillance and Reconnaissance –** Terrorist groups use drones to monitor enemy positions, track security forces, and plan attacks.
- **Suicide Drone Missions –** Similar to suicide bombers, drones can be programmed for self-destruct missions, targeting high-value assets or individuals.

Advantages of Drones for Terrorist Organizations

Several factors make drones an attractive weapon for terrorist groups:

- Drones can strike locations that are otherwise difficult for suicide bombers or vehicle-borne explosives to access.
- Chemical and biological payloads can cause large-scale casualties and devastation.
- Drones enable covert operations, offering terrorists the ability to launch attacks from unexpected locations.
- Modern drones allow accurate strikes without the need for direct human involvement.
- Compared to ballistic missiles and piloted aircraft, drones are significantly cheaper and widely available.
- Many current air defense mechanisms struggle to detect and neutralize low-altitude UAVs.
- The presence of drones creates fear among civilians and policymakers, making them a tool for coercion, intimidation, and negotiation.

The Impact of Drones and Robots on Traditional Terrorist Tactics and Strategies

The integration of drones, automated UAVs, and robotics has significantly altered military and terrorist tactics, reshaping the power dynamics between state and non-state actors. The following section explores these transformations.

A Shift in the Power Equation

The use of drones and robots has redefined warfare as a new social space where states and terrorist organizations engage in strategic confrontations. This shift has weakened traditional security structures, making conventional counterterrorism methods insufficient to address emerging threats. Previously, military and law enforcement agencies were able to engage extremist insurgencies directly. However, the increasing anonymity of insurgents, the scale of attacks targeting both civilians and critical infrastructure, and the ability to strike from hidden locations highlight the limitations of conventional military tactics.

Terrorists have leveraged drones and robotic technologies to reduce their dependence on human operatives, allowing for remote operations that minimize risks to their personnel. This shift fundamentally alters the nature of warfare, making conflicts more lethal and challenging to control.

The Role of Artificial Intelligence and Military Technology

The combination of artificial intelligence (AI) and autonomous warfare tools has profound implications for security and combat strategies:

- AI-driven drones and robots can identify, track, and eliminate targets with minimal human intervention.
- Surveillance drones provide real-time reconnaissance, improving operational planning.
- The use of automated weapons increases the precision and impact of terrorist attacks.
- Terrorist organizations can conduct large-scale attacks with fewer operatives.

Historically, advanced military technology was difficult to access, but the increasing privatization of warfare—through companies like Blackwater—and the commercialization of drone technology have made these tools more accessible. The ease of acquiring autonomous combat drones and "killer robots" has blurred the power balance between terrorist groups and government forces, enabling extremist organizations to challenge state security with unprecedented capabilities.

This evolution in warfare suggests a future where conflicts become even more automated, unpredictable, and destructive, necessitating new countermeasures to address emerging threats. Many writings have illustrated how communication technologies and the media have revolutionized various groups, as these technologies are actively used to collect funds, attract supporters, conduct operations, and disseminate activities. The use of drones by terrorists and their incorporation into operations and programs is just one branch of terrorism that benefits from modern technological advancements. On this basis, research and studies related to terrorism focus on monitoring how terrorism evolves with modern technology.

For this reason, studying the methods and areas that terrorists exploit technically would draw attention to the issue of drones. Tech-savvy terrorists utilize the latest technological innovations, including robotics, machine learning, and unmanned aerial systems. There is no doubt that this will spark numerous discussions regarding the sale and trade of drones and who can legally purchase them. If the movement of a drone, as any specialist knows, is not closely monitored, it becomes indistinguishable from the movement of a heavily armed tank within cities, residential neighborhoods, or near sensitive national installations and sites.

In this context, the United Nations has discussed the creation of no-fly zones around airports and critical UN installations. Additionally, companies have taken steps to develop geographic no-fly mechanisms and technologies that would automatically cancel, stop, or disable drone operations if they are detected flying in restricted areas. Given the complexity of these developments and the ways in which terrorists benefit from emerging technologies, it is expected that members of specialized international committees on counterterrorism will work on a final document outlining how terrorists exploit technology, along with measures to counter its actual and potential misuse. Countries are also expected to exchange updated information on recent developments, research, and best practices, in accordance with international human rights law, to address these threats. Their meetings will likely discuss joint initiatives through industrial cooperation, public-private partnerships, and legislative, policy, and regulatory measures.

Tactics and Strategies Used by Terrorists:

- Drones are deployed to gather intelligence on weak and exposed points. Their capabilities allow them to remain undetected during terrorist attacks.
- Drones can carry explosives and communication-jamming tools to disrupt state defense formations. Additionally, their use in swarms enhances coordination, increasing their lethality.
- Drones are used to capture photographs and videos of successful attacks to boost the popularity of terrorist organizations. Groups like Daesh have also utilized drones for propaganda purposes.
- Drones can be used to disrupt government infrastructure and major events, causing significant economic damage.
- Terrorist organizations exploit vulnerabilities in targets due to their ability to reach and attack them effectively.

Increased Accuracy and Effectiveness of Attacks and Challenges in the Fight Against Terrorism

Technological advancements and terrorists' ability to access dangerous technologies raise concerns about the measures and efforts needed to combat terrorism. Controlling trade, detecting, and monitoring the spread of these technologies are critical areas that countries and business entities must address. Commercial technology, as well as everyday objects and materials, have been transformed into dual-use technologies with military applications. This requires policymakers, businesses, and ordinary citizens to be aware of such dual-use technologies and their proliferation for war purposes, enabling them to make immediate decisions when necessary. However, this process can be hindered by disinformation, misinformation, or fake news, as ordinary citizens have access to various sources of news and information through social media platforms.

Another challenge in counterterrorism strategy is managing terrorists' access to commercial products and ensuring accountability at both collective and individual levels across political, media, commercial, and academic sectors. This issue is further exacerbated by counterstrategies employed by terrorist groups, which often

stay ahead of counterterrorism measures. Daesh, for example, has demonstrated its capabilities before nations could react and implement countermeasures. Bruce Hoffman argues that “the success of terrorists depends on their ability to stay one step ahead of the authorities, as well as counterterrorism technology.”

Moreover, laws governing the distribution of such technologies face challenges that can be exploited by both state and non-state actors, posing a significant hurdle for government authorities. The liberalization of commercial activities and human rights considerations make states more accountable than non-state actors. Terrorists, however, are not bound by these responsibilities and thus operate with relative impunity. Consequently, as impunity increases, so does terrorist activity, while legal constraints reduce the effectiveness of state countermeasures. In this context, the development of autonomous weapon systems by professional armies, such as those of the United States, the United Kingdom, France, Russia, and China, raises new concerns about the potential for non-state actors to acquire such systems. This has necessitated the establishment of laws to control the export of dual-use technologies and limit their illegal proliferation.

The acquisition of drones by terrorist organizations does not necessarily involve corruption, bribery, or dishonesty. Instead, it occurs openly, with certain countries facilitating the process, often in full view of the global community. For instance, the United States recently imposed new sanctions on 10 entities and four individuals located in Iran, Malaysia, Hong Kong, and Indonesia, accusing them of contributing to Iran’s drone production. According to the U.S. Treasury Department, this network facilitated the purchase of millions of dollars' worth of spare parts for the Iranian Revolutionary Guard Air Force and the Khad Kafeel Jihad organization, which is affiliated with Iran's drone program.

"Iran's production of deadly drones and their illicit proliferation through its terrorist proxies in the Middle East and Russia have heightened tensions," stated Brian Nelson, the U.S. Treasury Secretary for Terrorism and Financial Intelligence. Washington has long accused Tehran of supplying Russia with these weapons for use in Ukraine, but Iran has denied these allegations, asserting that Russia does not need Iranian industries and can acquire drones from the same commercial sources as Iran.

Drone attacks carried out by terrorist groups or militias unaffiliated with official state forces cause significant damage and can undermine the reputation of a country's armed forces, particularly if they are directly exposed to such attacks. One of the most striking examples occurred in Syria when a drone targeted a graduation ceremony at the Military College in Homs, prompting the Syrian Minister of Defense to leave. The Syrian Ministry of Defense confirmed that both civilians and soldiers were killed in the attack but did not name any specific organization responsible, and no group immediately claimed responsibility. As expected, images of panic and confusion spread rapidly following the sudden strike, showing civilians fleeing in terror and videos of injured individuals covered in blood. This highlights the severe impact such attacks have on a nation's military, security, and national stability, emphasizing the need for effective counterterrorism strategies. In response, Syrian forces launched airstrikes on areas in Idlib controlled by opposition activists following this attack.

Ethical considerations and legal violations of laws and international conventions

In recent contexts, the adoption of drones and robots by professional soldiers and non-state actors has sparked a debate on ethical and legal issues linked to their lethal nature, their uses, and their ability to kill autonomously. A drone system can be considered legal or illegal when used as an instrument of war, depending on the reasons for its use. Its ability to destroy homes and civilian targets is a source of concern. However, fighting between states can be considered a legal means of self-defense; conversely, it can be classified as extrajudicial execution or assassination. In this context, the Geneva Conventions of 1949 highlight the importance of addressing legal issues. Article 3 of these agreements deals with belligerent parties of signatory states but does not address the extent and intensity of hostilities.

According to some studies, since 2004, 114 drone attacks have been recorded in the northwestern regions of Pakistan, during which between 830 and 1,210 people were killed. According to reliable sources, between 550 and 850 of them were militants, representing two-thirds of the total casualties. Some researchers estimate that the real number of civilians killed in drone attacks since 2004 is about 32% in these regions. The killing of civilians in drone attacks is one of the most controversial issues in

Pakistan. These operations provoke discontent among the population, who consider them a violation of national security and sovereignty. In 2009, more than 700 civilians were killed in drone attacks, while an American official told *The New York Times* that only 20 civilians had been killed in two years, compared to 400 militants. Several influential commentators claim that the number of civilian victims of drone attacks in Pakistan could be as high as 98%.

It is worth noting that drones can kill civilians loyal to the state and opposed to terrorist organizations. Furthermore, the primary objective of state-led counterterrorism operations is to protect civilians from terrorists, not to kill more innocent people while pursuing enemies. These counterterrorism drone programs could become less controversial if their advantages and disadvantages were better explained. Academics and human rights activists suggest that international human rights laws and other relevant aspects of international law must be reconsidered. Despite the rapid development of unmanned aerial and ground vehicles, countries and international organizations seem to be content with existing laws and have not considered creating new ones. The principle that "the law must not follow drones; drones must follow the law" implies that combat instruments such as drones should be regulated based on general principles of international humanitarian law. Existing laws must be revised to define criteria for determining the limits of conflicts.

This issue is addressed by the Geneva Conventions, which form the foundation of humanitarian law. The Geneva Convention of 1864 deals with the impact of war on soldiers, while the Geneva Conventions of August 12, 1949, focus on the protection of war victims. The famous proverb *"Si vis pacem, para bellum"*—which means *"If you want peace, prepare for war"*—makes it difficult for states to adhere to a world governed by laws and rules. In this context, contemporary drone warfare has given rise to one of the biggest legal controversies.

If the human factor were completely replaced by machines capable of making decisions and starting wars, it could have a detrimental impact on human life. The issue is not autonomy itself but its impact on human life. Machine dependence on a human operator justifies human error, such as collateral damage, as human nature is not free from mistakes. However, if a machine error—whether due to faulty software

or a cyberattack—results in human casualties, the scenarios would be entirely different. Although drone system advocates claim precision, machines cannot match human capacity for evaluation and situational analysis.

The United Nations Security Council has taken steps to control drone systems to prevent their use by insurgents and terrorists. In 2017, Security Council resolutions condemned 23 types of weapons, including small and light weapons, military equipment, drone systems and their components, homemade explosive components, and other related materials. Member states were urged to prevent such systems and weapons from being acquired by groups such as Daesh, Al-Qaeda, and their affiliates, as well as other illegal armed groups and criminals.

Cooperation has been established between several organizations, including the United Nations Counter-Terrorism Executive Directorate, the United Nations Office on Drugs and Crime, the United Nations Institute for Disarmament Research, the International Organization for Migration, INTERPOL, the European Commission, and the Global Counterterrorism Forum. The Berlin Memorandum on Good Practices for Combating the Use of Unmanned Aerial Systems has been published. The United Nations Counter-Terrorism Office collaborated with the CAR project to study global trends in the use of unmanned aerial systems. In 2022, the European Commission completed the European Drone Strategy, which includes the development of a framework for drone operations and technical regulations. Efforts are underway in academia to design a robust system for monitoring drone technology.

Anti-Terrorism measures using Drones

Efforts to control drones have led to the adoption of various measures to combat drones and implement effective neutralization systems, the most important being geolocation technology, with drones guided by GPS satellites. The effectiveness of geo-restriction lies in its ability to prevent drones from entering restricted areas. However, the limitations of the integrated software are managed by the commercial companies that build the drones, and geo-restriction remains limited to sensitive locations and military bases only. It can also be bypassed when the owner does not

activate it or when attackers compromise the device. Wrapping aluminum foil around the GPS antenna can also prevent geofencing.

Secondly, radio interference can disrupt communication between the operator and the drone or disable the satellite positioning system. RF jammers vary in size, from small, rifle-sized devices to large jammers installed on vehicles and buildings. The system sends signals to override those from the GPS satellite or operator, causing the drone to lose its signal. As a result, it may either land or return to the designated landing site if it has been previously programmed. Jamming radio frequencies has proven effective in preventing drone attacks. However, each company develops unmanned aviation systems according to its own specifications, which are further customized by the end user to set the system and frequency of radio signals. This means that radio frequency jammers work differently for each drone.

Additionally, the output of RF jamming systems may interfere with other systems using radio signals between 2.4 and 5 GHz and GPS satellites. It can also have a negative impact on home security systems, transportation, and delivery services.

Thirdly, nets are used as a countermeasure, covering a large contact area against an incoming target, effectively engaging and disabling the drone's blades. Similarly, specially designed systems and even birds have been used to combat drones. However, they have a limited operational lifespan and are affected by terrain conditions, making them less reliable for drone countermeasures. Nevertheless, the presence of free birds, notably pigeons, which can detect noises and movements of unmanned aircraft, could be a useful measure. Additionally, marine mammals can be used to locate mines, equipment, and underwater intruders.

Conclusion

Drones and robots have become the tools of choice for terrorist organizations, sparking one of the biggest controversies related to warfare. The adoption of automatic UAV operational capabilities has reduced dependence on humans in wars. As a result, warfare has entered a post-human social sphere, where the actors involved coordinate their actions. Given that the possession of war equipment and capabilities is no longer limited to states alone, the trade of war and the liberalization

of technology have enabled terrorist organizations to acquire unmanned aircraft systems and robots relatively easily as tools of war. This capability has reduced the power disparity between non-governmental actors and states, allowing terrorist groups to inflict greater harm on any country.

This development has raised serious ethical and legal concerns. Some argue that while the use of unmanned aircraft systems by states on the battlefield may be legal, terrorist groups operate without regard for human rights and ethical considerations. In this sense, anti-terrorism measures against drones are hindered by states' inability to implement widespread surveillance techniques. Furthermore, the proliferation and commercial use of drones have facilitated terrorist groups' access to these systems. Although efforts are being made to control the spread of unmanned aircraft systems, achieving this goal is no small feat—akin to undertaking the "Mission of Hercules."

Recommendations for future research and counter-terrorism strategies

Three categories of policy recommendations can be developed. The first category concerns defensive measures, the second anti-attack measures, and the third preventive measures.

Defensive policy measures

- Develop interception technology that requires scientific research to detect, intercept, and automatically target drones. This can be achieved by investing in radar and anti-drone systems capable of neutralizing threats.
- Strategic, commercial, and large-scale sites must be equipped with anti-drone defense systems.

Dissuasive measures

- Track and trace drone operations and supply chains using human and technical intelligence. Intelligence techniques include reconnaissance, surveillance, signal detection, tracking, and satellite imagery. These efforts can be enhanced by transforming existing monitoring and reconnaissance systems into smaller, more

efficient intelligence and surveillance networks, requiring a highly skilled workforce.

- Countries must also strengthen human intelligence capabilities to track terrorist activities.

Preventive measures

- Develop an integrated tracking system for all drones, whether commercial or non-commercial. A unique identification number—similar to a mobile phone IMEI—could help authorities track drone operators.
- Integrate commercial drone sellers and buyers into a national identity database. Bank transactions related to drone purchases should be linked to national identification numbers.
- Monitor and regulate land, air, and maritime movements within the country and across borders. This requires strengthening review and investigation mechanisms.
- Enhance international cooperation and intelligence-sharing between countries.
- Develop global drone control systems, similar to international arms control treaties, to regulate drone technology and usage.

References

1. IG Shaw, 'Robot Wars: US Empire and Geopolitics in the Robotic Age' (2017) *Security Dialogue* 451.
2. TheoryTalk, 'Peter W. Singer on Child Soldiers, Private Soldiers and Robot Soldiers' (29 April 2009).
3. CJ Hall, *Essence of Diplomacy* (Palgrave Macmillan 2005).
4. IG Shaw, 'Robot Wars: US Empire and Geopolitics in the Robotic Age' (2017) *Security Dialogue* 451.
5. PW Singer, 'War of the Machines' (2010) *Scientific American* 56.

6. J Cartwright, ‘Rise of the Robots and the Future of War’ (21 November 2010).

7. PW Singer, ‘War of the Machines’ (2010) *Scientific American* 56.

8. IG Shaw, ‘Robot Wars: US Empire and Geopolitics in the Robotic Age’ (2017) *Security Dialogue* 451.

9. IG Shaw, ‘Robot Wars: US Empire and Geopolitics in the Robotic Age’ (2017) *Security Dialogue* 451.

10. A Rossiter, ‘The Impact of Robotics and Autonomous Systems (RAS) Across the Conflict Spectrum’ (2020).

11. ‘The Emergence of Lethal Surveillance: Watching and Killing in the History of Drone Technology’ (2016) *Security Dialogue* 1.

12. S Kreps, Democratizing Harm: Artificial Intelligence in the Hands of Non-State Actors (2021).

13. United Nations Office of Counter-Terrorism, Protecting Vulnerable Targets from Terrorist Attacks Involving Unmanned Aircraft Systems (UAS) (2022).

14. A Rossiter, ‘The Impact of Robotics and Autonomous Systems (RAS) Across the Conflict Spectrum’ (2020).

15. TG Pledger, ‘The Role of Drones in Future Terrorist Attacks’ (2021) *The Association of the United States Army*.

16. AI Aljuhani, *Drones (UAVs): Terrorist Groups’ Arms Race* (Islamic Military Counter-Terrorism Coalition 2023).

17. M Yaacoub and others, ‘[Full Citation Needed]’ (2020).

18. ZD Ice Ilijevski, ‘The Weaponization of Drones – A Threat from Above Used for Terrorist Purposes’ (2021).;S Kreps, *Democratizing Harm: Artificial Intelligence in the Hands of Non-State Actors* (2021).

19. United Nations Office of Counter-Terrorism, *Protecting Vulnerable Targets from Terrorist Attacks Involving Unmanned Aircraft Systems (UAS)* (2022).

20. P Chertof, *Perils of Lethal Autonomous Weapons Systems Proliferation: Preventing Non-State Acquisition* (Strategic Security Analysis 2018).

21. Addressing Risks from Non-State Actors' Use of Commercially Available Technologies' (2023).

22. P Chertof, Perils of Lethal Autonomous Weapons Systems Proliferation: Preventing Non-State Acquisition (Strategic Security Analysis 2018).

23. P Chertof, *Perils of Lethal Autonomous Weapons Systems Proliferation: Preventing Non-State Acquisition* (Strategic Security Analysis 2018).

24. Mateusz Osiecki and AF [Full Name Needed], 'Drone as a Target of Terrorist Attack and a Weapon Against Terrorism – Analysis in the Light of International Law' (2022) *Journal of Intelligent & Robotic Systems*.

25. Mateusz Osiecki and AF 'Drone as a Target of Terrorist Attack and a Weapon Against Terrorism – Analysis in the Light of International Law' (2022) *Journal of Intelligent & Robotic Systems*.

26. AI Aljuhani, Drones (UAVs): Terrorist Groups' Arms Race (Islamic Military Counter-Terrorism Coalition 2023).

27. A Rossiter, 'The Impact of Robotics and Autonomous Systems (RAS) Across the Conflict Spectrum' (2020).

28. TG Pledger, 'The Role of Drones in Future Terrorist Attacks' (2021) *The Association of the United States Army*.

29. DC Liang, 'Preventing Terrorists from Using Emerging Technologies' (2023) *Vision of Humanity* https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies/