

AI warfare and human rights: Accountability and global implications in armed conflicts

Tarik Hodzic^{*}, Sai Khun Min (Arthur)^{**}, Zai Aurangzaib^{***}, Euloge Koffi^{****}, Rachel Cantlow^{*****}, and Abdulrahman Subih^{*****}

Abstract: *This paper examines the accelerating integration of artificial intelligence (AI) systems into contemporary warfare and its implications for international humanitarian law (IHL), human rights, and corporate accountability. The analysis traces how AI systems have rapidly shifted from experimental tools to central components of global military operations, developing from tools of surveillance into tools of autonomous killing. Despite their growing influence, military applications of AI remain exempt from major regulatory frameworks, one of them being the European Union Artificial*

^{*} Tarik Hodzic is an alumnus of the University of Auckland, Massey University, and the Global Campus in South-East Europe (ERMA). He currently works for the German Agency for International Development in Sarajevo, Bosnia and Herzegovina, helping sustain independent media in the Western Balkans.

^{**} Arthur is an LGBTQIA+ rights researcher from Myanmar. He came from an international relations background and worked on cultural diplomacy for over a decade. His current research projects focus on LGBTQIA+ discrimination and acceptance, systemic sexism, intersection of religion and gender, and anti-gender movements in the Southeast Asia region.

^{***} Zai Aurangzaib is an alum of the Master of Arts in Human Rights and Democratisation in Asia Pacific (GC APMA) and the United States Department of State. They are the co-founder of Trans Masc Alliance Pakistan, a community-led organisation advancing SOGIESC inclusion and gender diversity across South Asia.

^{****} Euloge Koffi holds a LLM in Human Rights and Democratisation in Africa and serves the African Commission on Human and Peoples' Rights as a Legal Associate.

^{*****} Rachel Cantlow is an alumna of the OSCE Academy in Bishkek, where she earned a Master of Arts in Human Rights and Sustainability. She previously served as Liberation and Campaigns Assistant at Leeds University Union and has worked to advance human rights, inclusion, and community engagement.

^{*****} Dr. Abdulrahman Subih is an international law scholar and Ph.D. graduate from Dr. Babasaheb Ambedkar Marathwada University. His research focuses on the international laws of technology transfer, human rights, and positive psychology. He writes about how global legal frameworks, new technologies like AI, and ethics impact people worldwide.



This article content is offered under a [CC Attribution Non-Commercial No Derivatives license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

©2025 the Authors

Intelligence Act, creating a legal vacuum in which States and private companies develop and deploy high-risk systems without binding oversight. By taking a regional approach, drawing on case studies from Europe, the Middle East, Southeast Asia, South Asia and Africa, the paper highlights the increasing privatisation of warfare, where technology corporations, including Google, Microsoft, Palantir, Huawei, and regional actors, including the US, Russia, China, Israel, supply data infrastructure, targeting software, and autonomous capabilities that blur traditional boundaries of responsibility. The Ukrainian conflict demonstrates how AI-driven drones, decision-support software, and public-private collaboration has transformed battlefield logistics and targeting while eroding meaningful human control. In Gaza, Israeli systems such as Lavender, the Gospel, and Where's Daddy? illustrate how algorithmic target generation, often with minimal human verification, raises acute concerns regarding distinction, proportionality, and precaution under IHL. Meanwhile, conflicts in Myanmar and across Southeast Asia, and South Asia show how AI-enabled surveillance and weapons proliferate through opaque defence partnerships involving China, Turkey, and Russia. Across these contexts, the paper argues that AI systems magnify existing accountability gaps by distributing decision-making across programmers, corporations, and military actors, making attribution for unlawful harm increasingly difficult. The study concludes that without robust regulation addressing both State and corporate obligations, AI-driven warfare risks normalising systemic violations of human rights and accelerating the erosion of established norms governing the use of force.

Keywords: AI systems; human rights; business accountability; automation; conflict

1. Introduction

In 2020, during the final months of Libya's civil war, reports emerged of what is now considered the first instance of an artificial intelligence (AI) system autonomously engaging human targets. According to a United Nations (UN) panel of experts, a Turkish-made Kargu-2 drone operated without direct connectivity to a human controller, attacking retreating forces of the Libyan National Army and inflicting casualties. This drone was publicly marketed as a "combat proven" and cost-effective weapon by STM, a private company created by the Presidency of Defence Industry of the Republic of Türkiye. The incident marked a pivotal shift in the conduct of warfare, foreshadowing a transition from human-directed combat to conflict driven by algorithm-based weapons and technology, evident in the conduct of modern conflicts across the globe. At the heart of this transformation lies the intersection of State military ambitions, international legal obligations, and the profit-oriented motives of private and State-owned defence and technology industries.

In the years since Libya, a rapidly expanding war-tech industry has transformed AI systems from a theoretical tool of efficiency into an integral component of the global war industry. What began as experimental

automation in logistics and reconnaissance has evolved into a multibillion-dollar sector linking governments, private weapons manufacturers, and major technology companies. By processing vast quantities of data, AI systems now underpin surveillance, intelligence gathering, and increasingly, decision-making in the use of weapons ranging from drones to missiles.

The growth of this unregulated military and corporate partnership illustrates the ever-growing privatisation of the war industry. Governments now depend heavily on private companies for AI system development, deployment, and maintenance. Major technology firms such as Google, Amazon, Microsoft, Palantir Technologies, and OpenAI have signed multi-billion-dollar contracts to supply military grade AI infrastructure. Under Israel's Project Nimbus, for example, Google and Amazon provide cloud computing and AI services used in military operations in Gaza. Similar collaborations involve Dell, Cisco, and IBM's Red Hat, which furnish data processing infrastructure and analytical tools to defence networks. These commercial partnerships enable States to outsource both innovation and accountability, creating a diffuse system of shared responsibility in which no single actor bears full legal or moral liability for the consequences of AI-assisted warfare. As *Time* reports, the changing nature of warfare stands to give private technology companies greater power as independent actors than at any time period before, emphasising that those companies willing to move fastest without ethical or regulatory norms stand to gain the most out of the current war industry ecosystem (Serhan 2024).

The European Union's Artificial Intelligence Act (2024) defines AI systems as "machine-based systems designed to operate with varying levels of autonomy," capable of learning from data to produce outputs, such as "predictions, recommendations, or decisions", that influence physical or virtual environments. Yet the same regulation explicitly excludes military, defence, and national security applications from its scope (Recital 24), regardless of whether such systems are developed by public or private entities. This exemption has created a legal vacuum in which the defence sector, precisely the field where the stakes are highest, remains outside the reach of civilian oversight. It allows AI technologies originally designed for civilian purposes to be repurposed for combat without any binding obligations of transparency, ethical review, or explicit accountability under international law.

From a human rights standpoint, this evolution raises serious concerns. Algorithmic surveillance, predictive targeting, and automated strike decisions bring into question accountability with long standing tenants of international law. For instance, misidentification between combatants and civilians due to a flawed recognition system could lead to violation of the principle of distinction (Additional Protocol I, Article 48), whereas AI systems may also fail to assess whether expected civilian harm outweighs the

anticipated military advantage, breaching the principle of proportionality (Additional Protocol I, Article 57) (Kallenborn 2021). Moreover, when AI systems are trained on data reflecting social or political biases, they may systematically discriminate against particular ethnic, religious, or social groups, violating the right to equality before the law (ICCPR, Article 26), while further decisions making without human approval could lead to circumstances where lethal force is not strictly necessary, violating the right to life (ICCPR, Article 6). The fear of such events taking place in the future led UN Secretary-General António Guterres to warn in 2025, “machines that have the power and discretion to take human lives without human control should be prohibited by international law. We cannot delegate life-or-death decisions to machines.”

Legally, the situation remains precarious. As the International Committee of the Red Cross (ICRC) notes, autonomous weapons and AI systems are not explicitly regulated by existing treaties. Responsibility for compliance with international humanitarian law (IHL) rests with human commanders and operators, who must maintain “meaningful human control” over targeting decisions. As AI systems grow increasingly complex, however, the chain of accountability becomes difficult to trace. Programmers, corporate developers, and military decision-makers each play roles in systems that can act faster and less predictably than any human operator.

The Convention on Certain Conventional Weapons (CCW) continues to debate these issues through its Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS). Despite years of discussion, no consensus exists on definitions, yet alone limits. According to Michal Onderco (2025), while countries in the Global South have pushed for the development of binding international norms, leading powers such as China, Russia, and the United States remain sceptical of regulation and have repeatedly hindered progress in creating enforceable legal rules. Onderco (2025) further notes that we are currently in a state of “latency,” where States possess all the technological elements necessary to build fully autonomous weapons systems but have not yet made the political decision to deploy them. In other words, the capability already exists, but the threshold decision simply has not yet been taken.

Meanwhile, commercial actors expand development at a pace that outstrips diplomacy. Analysts predict that within ten years, AI will become the dominant “military vector,” shaping both strategy and battlefield conduct (De Vynck 2023). The result is a widening regulatory gap between the ethics of warfare and the economics of war, with no outright responsibility or obligation explicitly present in the doings of private companies and the business side of the equation which holds power in the production and dissemination of this technology to emerging war parties. The emergence of these technologies, and their subsequent engagement in a conflict zone, brings questions of responsibility and accountability,

especially in the context of human rights violations. The following writing will address these concepts with the goal of identifying evident patterns of use of AI systems in warfare around the globe, aiming to illustrate the ever-increasing need for recognition of the relationship between business, Governments, and their joint responsibility towards human rights obligations, or the lack thereof. This will be done through the prism of international conflicts, from the Russian invasion of Ukraine, various conflicts in Africa and Southeast Asia, to the ongoing genocide Israel is perpetrating in Gaza.

2. European context

February 2022 saw a pivotal event for Europe, and for the dawn of integration of AI technology into the war industry. What started off as an attempt by Russia to quickly invade and control the key points of Ukraine including Kiyev, quickly became a war of attrition akin to the Western Front of World War I. From a war marked by quick movement of soldiers and equipment, the current state of relations in Ukraine are dominated by technology, and in particular AI driven drones. David Kirichenko (2025), a specialist on warfare, specifies that currently drones constitute upwards of 80 percent of casualties on the Ukrainian front, whereas human and other equipment account for less than 20 percent. In the hundreds of thousands, drones and other AI based technology flood the fields of Eastern Ukraine, constructing a nexus of interwoven actors, from Government agencies and their procurements, to companies and startups filling the needed technological gaps in order to produce the adequate answer to Russian aggression. Although fully autonomous weapons have not yet appeared on the battlefield, current demonstration and intent expressed by high ranking military officials point toward increased automation and a reduced role for human oversight. The Ukraine war, therefore, acts not only as a geopolitical confrontation, but a live experiment in the militarisation of AI and the privatisation of warfare.

The information gathered by drones employs AI systems to process vast amounts of data, subsequently pipelined in a way that enables easier identifying of enemy positions, mapping of movements, and launching coordinated responses by the Ukrainian Armed Forces. Though this does not present an intrinsic violation of human rights, the integration of AI systems into unmanned aerial vehicles (UAVs) has been particularly transformative. The Receptor AI, a product of company Quantum Systems, enables Vector drones to lock onto a target and fly autonomously for the rest of the mission (Quantum System 2024). These drones are only starting to unlock their potential, as they are being repurposed from reconnaissance tools into strike platforms (Mamediiieva 2025). This, however, is only the precursor to the plans of current military heads. As Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, explained, the country is deliberately pursuing what he calls a "tech war," striving

for “full autonomy.” According to Fedorov, Ukrainian developers are “training models to recognise targets and understand target prioritisation,” with humans still intervening where necessary but “developing different scenarios for taking autonomy further.” He further revealed that “some autonomous drones, which we have not announced, have a high degree of autonomy and can potentially combine themselves into swarms,” signalling Ukraine’s commitment to pushing the technological frontier towards automatised warfare (Boffey 2025).

On the Russian side, similar innovations are emerging. Russian military experts have publicised the use of the Lancet-3 loitering munition, produced by ZALA Aero Group, which employs convolutional neural networks to analyse video content during flight, autonomously detecting and classifying enemy targets before transmitting coordinates to attack drones (Pardo de Santayana 2024). Moreover, recent reports by Ukrainian intelligence detail the implementation of AI systems in the V2U Russian drone capable of autonomous decision making. As Beskrestnov explains, “(V2U) navigates autonomously and attacks the target autonomously” (Maksymiv 2025). This integration of neural networks into battlefield operations demonstrates that both sides are relying on AI systems to accelerate combat decisions and reduce human response times.

With extensive United States assistance, Ukraine has become a laboratory for testing emerging AI systems under real combat conditions (Flournoy 2023). Boffey (2025) describes the conflict as being “at the forefront of the global AI and drone revolution.” This has created a form of asymmetric innovation, where necessity and resource constraints drive the rapid adaptation of commercial technologies for military use, without much care for the rules and regulations which may guide it toward human rights and responsible business regulation.

From the outset, much of Ukraine’s AI innovation was driven by volunteer networks and start-ups rather than State institutions. Firms such as Lookery, Respeecher, and Augmented Pixels initially spearheaded AI-driven solutions before government agencies began building their own capabilities (Bondar 2024). The State later institutionalised this collaboration through initiatives like the Brave1 platform, which provides grants of up to \$30 million USD to over 1,500 technology firms engaged in AI and defence production (Kuzio 2025). This ecosystem fosters an unprecedented degree of public-private partnership, enabling rapid prototyping and deployment of military technologies. The Ministry of Digital Transformation has explicitly refrained from regulating AI in the defence sector, arguing that flexibility and speed are essential for wartime adaptation (Bondar 2024). Consequently, more than 500 private defence companies now operate independently of direct State control, producing a range of AI-driven drones and automated systems. The defence company Swarmer, for example, has developed software that allows drones to

autonomously prioritise targets, while DevDroid produces AI-assisted machine guns that detect and track human movement, though automatic firing remains disabled due to friendly-fire concerns (Bondar 2024; Abdurasulov 2025).

At the same time, foreign technology firms play a critical role. American companies such as Palantir Technologies, Google, Amazon, and Microsoft have all provided AI infrastructure to the Ukrainian military. Palantir's data integration software, for instance, enables battlefield commanders to visualise and predict enemy activity based on aggregated intelligence inputs (Bergengruen 2024). These partnerships have blurred the boundaries between commercial and military enterprise, granting private actors unprecedented influence over the conduct of warfare, with Bergengruen (2024) noting, "those willing to move fast and flout legal, ethical, or regulatory norms could make the biggest breakthrough."

Multiple actors are implicated in the deployment of autonomous systems, including programmers, software developers, hardware manufacturers, military commanders, and operational soldiers. Each of these actors contributes to the functioning of the system, yet no single entity can be held fully responsible when an autonomous system malfunctions or makes erroneous targeting decisions (Pardo de Santayana 2024; Abudrasulov 2024). This creates a responsibility gap in which violations of IHL, such as breaches of the principles of distinction, proportionality, or necessity, may occur without a clearly identifiable accountable party.

Accountability, thus, is blurred and beyond recognition. State parties and private actors are interwoven, there is no regulation which guides the production and implementation of these systems, other than the ever-collapsing international human rights framework. Although Ukraine maintains a "human-in-the-loop" approach requiring human approval for lethal decisions, the speed and autonomy of these systems increasingly erode meaningful human control. As scholars have observed, when operators merely press a button to approve strikes recommended by AI, their involvement becomes largely reflexive, leaving limited room for ethical judgment (Onderco 2025). Private-sector involvement further complicates accountability. Ukrainian and foreign technology firms provide critical infrastructure, AI models, and data analytics for military operations, yet they are often insulated from legal responsibility under both domestic and international law (Bergengruen 2024; Kuzio 2025). For example, Palantir Technologies provides software that predicts enemy movements, and companies like Swarmer and DevDroid develop autonomous targeting systems. While these firms facilitate military effectiveness, their status as commercial entities operating in collaboration

with the State blurs traditional boundaries between civilian and military responsibility (Bondar 2024).

As De Vynck (2023) notes, AI is poised to become the dominant military vector within the coming decade putting an emphasis on the growing centrality of software, data processing, and algorithmic optimisation in modern warfare. The conflict also demonstrates the evolving nature of military-industrial collaboration. Ukraine's AI systems benefit from a combination of volunteer initiatives, start-ups, and State-supported platforms which facilitate rapid prototyping, testing, and deployment (Kuzio 2025). This model accelerates technological development but simultaneously introduces new risks, as private actors gain outsized influence over operational capabilities and strategic decision-making. As the proportion of AI-enabled drones continues to rise, projected to reach 90 percent by the end of 2025, the distinction between algorithmic recommendation and autonomous action becomes increasingly blurred (Kuzio 2025; Kirichenko 2025).

3. Middle East context

The emergence of the Middle East as a primary AI conflict lab has created a regulatory challenge for the lawmakers. This challenge allowed more deployment of advanced military AI-based technology. The best examples are the Israeli AI supported systems such as Lavender and Gospel which serve as important case studies that show the lack of accountability. Lavender is an automated system made to identify the targets by increasing the speed of operation, make it difficult to hold the violator responsible and scatter the accountability between private developers and the State.

3.1. AI-driven targeting vis-a-vis accountability

After October 2023, the Israeli army deployed the AI-driven systems to target individuals in Gaza which does not align with IHL principles, in particular, principles of distinction and precaution.

On one hand, Lavender and Gospel function by creating a list of individual targets in a short time lacking sufficient human verification. Israeli forces totally rely on AI-generated lists to execute their missions bypassing the principle of precaution behind where humans do the meaningful verification.

On the other hand, the principle of distinction, which is heavily human in nature, is entirely given to a machine algorithm to distinguish between what is a target and what is not. This shift makes holding a specific actor accountable in case of legal violation, i.e., State, private actor, developer, and mission operators.

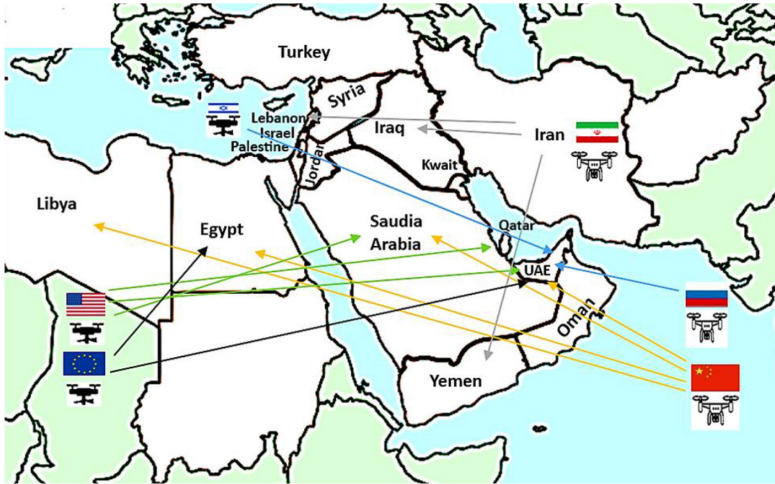


Figure. 1: Defense based AI and ML trade transaction in the Middle East (Traders & Customers). Source: Authors' own creation.

3.2. The use of AI decision-support systems by Israel

With the development of AI, the defence sector is likely to see a new kind of arms race for the dominance of these technologies that inevitably change warfare tactics and norms (Garcia 2019). the role and use of AI systems in the war in Gaza played a significant role in the unfolding genocide, with some scholars identifying this as the “first AI-powered genocide” (Fazi 2024). Key Artificial Intelligence Decision-Support Systems (AI-DSS) have been used in a number of ways and have enabled the Israeli Defence Forces (IDF) to substantially increase the scale of its operations and thus, the scale of civilian death and destruction (Dorsey and Moffett 2025).

The main AI systems under examination are Lavender, The Gospel, and Where's Daddy? The Lavender system is an AI-driven database designed to identify suspected members of Hamas by conducting its own analysis of surveillance data to generate targets (Andersin 2025). The Gospel system focuses on operational targeting by rapidly generating recommendations for buildings and structures where militants might be active, suggesting appropriate munitions based on previous target categorisations (Abraham 2024). Lastly, Where's Daddy? uses phone-tracking technology to monitor militants' movements, especially targeting them when they return to their homes, which is a tactic that supposedly confirms their presence and identity (Cvetkovič 2025).

These AI-DSS have significantly accelerated target production beyond human capability (Dorsey and Moffett 2025), aiding faster military responses on a scale that was never seen by human Israeli intelligence services in previous conflicts (Abraham 2023). More broadly, it has been

found that within the use of AI-DSS, there is often very little human intervention or verification (Holland 2024; Abraham 2023), resulting in a lack of certainty as to whether the AI system is analysing the data and identifying legitimate targets accurately (Dorsey and Moffett 2025). It has been reported that the only “check” of these AI generated target lists is a determination of whether the target is male (Serhan 2024).

Furthermore, the use of these systems represents a level of automation in warfare that poses serious ethical and legal challenges, with concerns over precision, civilian casualty and the risk to civilian infrastructure such as hospitals, residential buildings and schools, largely due to the speed at which AI-DSS produce targets, the data they use to do so, and the bias that they possess (Dorsey and Moffett 2025).

4. Southeast Asian context

With AI, the militaries around the world have transformed the way they think as well as how they operate, including the countries in South Asia and Southeast Asia region. Powered by AI, unmanned military systems can lower operational costs and political threshold therefore, the use of AI in the defence sector becomes inevitable for most countries (Rahman 2026). Due to being one of the leaders in AI technology as well as its geopolitical influences, China and Chinese tech companies have become the major exporter of AI in the defence sector in the Southeast Asia region.

Countries in the Southeast Asian region are at various levels of technological advancement and economic development. Despite this uneven playing field, the Association of Southeast Asian Nations (ASEAN) has its own policies and guidance on the use of AI, such as the ASEAN guide on AI governance and ethics, working group on AI governance, and ASEAN AI responsible roadmap (2025–2030). ASEAN defence ministers also note the incorporation of AI technologies in the defence sector of its Member States as well as accountability and responsibility in accordance with international laws (Ministry of Defense 2025). Plans for accountability for the use of AI are positive news; however, it is impractical due to its reference to existing international law and the existing gap in international law on the ethical use of AI in the defence industry. One key point that has been mentioned multiple times in ASEAN AI policies is urging the government to support AI start up on both national level and regional levels (ASEAN 2024a; ASEAN 2024b). In other words, ASEAN is trying to promote the role of private actors within the integration of AI in ASEAN.

The use of AI in the defence sector can be seen in two different ways in the southeast Asian region, in the form of lethal autonomous weapons and non-combat functions such as surveillance. Although there are no definitive proof of the use and the existence of AI-powered autonomous weapons within the region, the Philippines has the human resources to

further develop AI systems that can be used in autonomous weapons, and Singapore is the leader in the development of AI within the region (Austero and Savage n.d.). For example, starting from August 2025, Singaporean soldiers received training on the use of AI-powered drones (Rahman 2026). In terms of Thailand, the Royal Thai Army initiated the process of integration of AI into defence; however, it is still in the early stages (Bunnag 2022).

The use of AI in non-combat situations as well as the influence of China can be seen in the conflict in Myanmar. The coup in 2021 rekindled multiple decade-long civil wars between ethnic groups and the military (Chambers and Cheesman 2024). The Myanmar military has had long-standing relations with China, especially in the form of technological support. There are three main companies currently supplying military equipment and technology to the junta. Norinco, a State-owned defence corporation from China, has been working with Myanmar's military as early as 2017, with the goal of expanding defence cooperation in Myanmar. Wanbao, which is a subsidiary of Norinco, also supplied 5 to 10 million dollars' worth of goods to the junta in the years 2021 and 2022 as well (Irrawaddy 2025). China is supplying the junta not only with weapons such as drones, missiles, and even fighter jets but also training military officers in arms manufacturing as well (Thura 2025; Aye 2024). The third group of Chinese companies supplying AI power technologies for surveillance and Internet censorship includes Huawei, Danhua, and Hikvision. They are not directly communicating with the Junta, but through two local tech companies called Fisca and Naung Yoe. Danhua and Huawei are mainly providing CCTV cameras to ten different cities in Myanmar, and technology from Hikvision has been used in control rooms (Potkin 2022).

The main usage of AI in the Myanmar conflict is through AI-powered facial recognition and surveillance systems. Although Myanmar received fighter jets and UAVs from China, such as the FTC-2000G and CH-3 and CH-4, most of them are not fully autonomous (Matamis 2025). AI-powered surveillance systems have been used in Myanmar in order to track and identify the opposition (Köckritz 2025). It has also been used for internet and social media censorship as well as location tracking through mobile networks (Graceffo 2025). The companies that are responsible for internet surveillance in Myanmar are Mascots Group from Myanmar as a broker and Tiangou Secure Gateway and Geedge Networks from China (Myanmar n.d.). From AAPP's database (Assistance Association for Political Prisoners), among 2,812 recorded cases, a minimum of five cases were arrested due to something they posted on social media (AAPP 2025).

The use of AI in the defence sector in the ASEAN region is highly privatised. The use of AI in autonomous weapons or non-combat situations is carried out or procured through private companies mainly due to the lack of human resources as well as knowledge to create AI models within

the region. With the push through ASEAN AI policies, the role of private actors is going to be increased in the future.

While the ASEAN region is distinguished by the expanding role of private actors in AI-enabled defence, South Asia demonstrates how AI is already altering interstate military conflict.

4.1. South Asia, India-Pakistan conflict

India and Pakistan, the two nuclear States, have the most recent technologically advanced conflict in war history that has the most profound impact on South Asia and world politics. India launched a cross-border strike into Pakistani territory, named Operation Sindoor, on 7 May 2025, and used AI extensively to help target nine locations in Pakistan. During the operation, the Indian military combined real-time sensor data with 26 years of historical military records using roughly 23 locally built AI-driven applications to achieve a 94 percent accuracy rate (Sareen 2025).

After Pakistan shot down French Rafale planes imported by India, Rafale's stock reportedly fell, while Chinese defence manufacturer AVIC Chengdu Aircrafts' stocks rose up to 36 percent (Singh 2025). Both States deployed drones, loitering munitions, and surveillance platforms, aided by AI, marking this episode as one of the most technologically advanced conflicts in South Asia's history.

During the conflict, India claimed it used Israeli defence and aerospace UAVs, like Searcher and Heron, and Harop loitering munitions. It is also adding General Atomics Aeronautical Systems, Inc U.S.-made AI systems with the coming MQ-9B Predator. India has also used home-grown Aeronautical Development Establishment (ADE) UAVs, Dornier Rustom2, and Nagastra1. Pakistani drones were mainly from Turkish Aerospace Industries (TAI) and Chinese defence manufacturer AVIC Chengdu, like Bayraktar and Wing Loong II (Sareen 2025). Songar drones, reportedly used in May, further highlight China as a rival to European, Israeli, and United States private companies' military tech. AI-driven multisensor systems let operators quickly collect and rank targets with high strike success, according to military officials who confirmed AI use after the conflict (Philip 2025). This level of automation is unprecedented in the region and marks a trend toward algorithmic warfare, in which machines, not humans, influence life-and-death choices.

The use of AI and semi-autonomous systems also makes accountability harder (Shahzad 2024), since most targeting software and hardware comes from defence firms like Chinese defence manufacturer AVIC Chengdu, Israeli defence and aerospace, French Rafale, Turkish Aerospace Industries (TAI), and the General Atomics Aeronautical Systems, Inc U.S.

India's reliance on Israel and United States private corporations, and Pakistan's strategic military alliance with China and Turkey, have made this entire India-Pakistan conflict a foreign defence private company weapon exhibition with stock market reaction. The comparison between Rafael and Chinese defence manufacturer AVIC Chengdu during this conflict not only highlights China's advancements in technology and defence weaponry, but it also shows China's ability to compete with private European, Israeli, and United States defence corporations.

5. African context

The global discourse surrounding AI in warfare frequently centres on highly developed geopolitical arenas, yet the African continent provides an indispensable analytical frame for examining the legal, ethical, and accountability dimensions of these emerging technologies. These challenges include fragile State investigative capacities, opaque transnational military supply chains, the operational proliferation of non-State armed groups, complex external State interventions, and corporate opacity.

The operational landscapes of the Democratic Republic of Congo (DRC) and Sudan illustrate how advanced remote platforms interact with existing structural instability. In the DRC, the ongoing conflict mainly involves the Congolese national army and its aligned militias fighting the March 23 Movement (M23) rebel group (Armed Conflict Location & Event Data Project, ACLED 2026). The DRC Government accused Rwanda of declaring war after supporting the rebels with troops, leading to a peace agreement in June 2025 calling for the withdrawal of Rwandan troops and the cessation of support for rebel factions. But Rwanda still denies any support given to the M23 and nothing is yet effective from this peace agreement (Nantulya, Paul, 2026). This backdrop of disputed attribution and cross-border tension directly feeds into the broader accountability gaps surrounding drone procurement and deployment in the region.

The conflict in Sudan began in April 2023 as a power struggle between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF). The fighting devastated the capital Khartoum, the Darfur region, and other areas, causing a severe humanitarian crisis. With the involvement of international actors such as Iran and the UAE, the RSF has been accused of committing atrocities, including ethnic cleansing (Human Rights Council 2025, 11). The SAF regained control of key territories, including Khartoum in early 2025, but the war continued without a lasting ceasefire. The roots of the conflict lie in Sudan's history of instability, military coups and unresolved tensions following the 2021 coup, and disputes between the SAF and RSF forces over integration (Ayferam 2023).

Analysing the deployment of AI in Africa requires addressing a fundamental connectivity paradox. The continent remains less digitalized

than other global regions, with internet penetration in conflict-affected spaces like Sudan falling below 20 percent (Allen and Okpali 2022). This limited digital infrastructure directly impacts the accountability landscape. Low internet penetration severely restricts the capacity of local populations to access early-warning systems, hinders civil society from documenting IHL violations in real-time, limits access to digital evidence repositories, and obstructs the tracking of automated military assets. Despite these infrastructure constraints, AI-assisted weapons and remotely piloted systems are actively deployed in both theatres, but there is no public, well-documented evidence of the deployment of fully autonomous weapons. Instead, these conflicts rely on drones and AI tools that enhance human decision-making, support surveillance, and streamline logistics, while human operators retain control of targeting and engagement (Kuele 2015; Rahmtall 2025).

The risk of lethal consequences and human rights violations from AI-assisted or autonomous elements, even if not fully autonomous, remains a major concern. Sensor misreads, falsified GPS data, or software glitches can lead to erroneous targeting decisions or unintended escalations, thereby undermining IHL's requirements of precaution, distinction, and proportionality ((UN General Assembly 2024, 3). Indeed, for the African Union, IHL applies to all forms of warfare and to all kinds of weapons (Helal 2024, para. 47). While IHL functions as the primary *lex specialis* during active hostilities, IHRL remains concurrently applicable, especially Articles 1, 4, 5, 6, 16, and 18 of the African Charter on Human and Peoples' Rights (African Charter), the 2023 Resolution of the African Commission on Human and Peoples' Rights on Business and Human Rights (ACHPRBHR), and the United Nations Guiding Principles on Business and Human Rights (Guiding Principles).

Field evidence from both the DRC and Sudan demonstrates that the rapid acquisition of drone technology by State and non-State actors has resulted in widespread civilian casualties. Reports indicate that between 2023 and 2024, the DRC acquired nine CH-4 drones capable of launching bombs, and in 2025, Wing Loong II combat drones from Catic, a Chinese company (Mmilitär Aktuell 2025). In 2024, the local militia group Wazalendos, a militia Group used "suicide drones" carrying improvised explosive devices to launch attacks against United Nations peacekeepers (Bah 2024, 3). More recently, on 25 January 2024, around 20 civilians were killed in the town of Mweso, but the M23 and the Government army accused each other of launching the strike (Reuters 2024).

In Sudan, fleets of drones including Turkish TB2s and other platforms are operated by crews and command centres on the ground. Sudan has built a Kamin-25 loitering munition drone (Africa Defense Forum 2025, 13) and on 11 October 2025, the RSF launched a drone strike on a displacement shelter at Dar al-Arqam, killing at least 57 people,

including 22 women and 17 children. According to the World Health Organisation Chief, a drone attack on a hospital in Sudan's North Darfur region killed more than 70 people in January 2025 (Reuters 2024). Moreover, the United Nations Children's Agency documented the killing of 11 children by a drone strike on a mosque during prayers (Arab News 2025). Yet, manufacturers and financiers of drone systems supplied to the DRC and Sudan have conducted minimal public due diligence, with little transparency regarding risk assessments or mitigation of potential violations (Verbrugge et al., 16; Turkish Minute 2025).

The deployment of AI warfare in Africa underscores the volatile intersection between advanced military technologies and significant accountability gaps. Addressing this divide requires leveraging international legal frameworks such as the African Charter and the policy organs of the African Union to rigorously enforce transparency across corporate supply chains as part of a broader transitional justice process. Unless the legal responsibilities of manufacturers, brokers, and financial actors are clearly defined and bound to enforceable remedy mechanisms, the integration of automated military technologies will continue to exacerbate civilian suffering in armed conflicts.

6. International law and accountability for private actors

The rapid growth of AI and the involvement of private actors such as tech companies can be seen in every region around the world. This raises a question of who would be the responsible party for the hallucinations or mistakes caused by the AI system. As AI systems evolve toward self-directed operation, it becomes unclear who should be held liable when autonomous systems make errors: the programmer, the manufacturer, or the military user. One of the most relevant international laws for the use of AI in the defence sector would be IHL. The basic principles of IHL include precaution, distinction, and proportionality (UN General Assembly 2024, 3) which has been undermined by the use of AI in the defence sector.

The sole reliance on the AI outputs would not meet the distinction or precaution criteria under IHL. Distinction refers to the principle that "it is necessary to distinguish clearly and objectively the combatants from civilians" (Garcia 2019, 6), whilst precaution is the principle that "before any attack, the parties to the conflict must verify and ensure that the target is neither a civilian one nor subject to special protection" (ibid.). The examples of failure to adhere to the principles of distinction and precaution can be seen both in European context as well as the middle east context.

Due to the lethal consequences of AI-assisted systems, even if not fully autonomous, it remains a major concern. Sensor misreads, falsified GPS data, or software glitches can lead to erroneous targeting decisions or unintended escalations. Automated misidentification between combatants

and civilians, algorithmic bias, or errors in predictive targeting could violate both IHL and human rights law, without clear avenues for redress. Furthermore, the ICRC continues to emphasise “meaningful human control,” but this principle lacks concrete legal enforcement mechanisms.

In terms of regional mechanisms, it varies based on region by region. For the African Union, IHL applies to all forms of warfare and to all kinds of weapons (Helal 2024, para. 47). While IHL functions as the primary *lex specialis* during active hostilities, international human rights law remains concurrently applicable, especially Articles 1, 4, 5, 6, 16, and 18 of the African Charter, the ACHPRBHR, and the Guiding Principles.

The Guiding Principles have several loopholes for accountability. Similar to the rest of the international laws, it puts the responsibility on States in order to create domestic legal mechanisms that require enterprises to respect human rights. Furthermore, international or transnational enterprises are not a party to international treaties, therefore, they are not legally bound by the international laws. Existing international legal mechanisms are not designed for the businesses. Moreover, domestic legal mechanisms are still lacking in the countries where AI has been incorporated in the defence sector. Neither Ukraine nor Russia has established a domestic legal framework governing the military use of AI, leaving a regulatory vacuum that allows experimentation with minimal oversight (Oliinyk 2025).

7. Conclusion

The increasing integration of AI systems into warfare marks a transformative moment in the conduct, ethics, and accountability of armed conflict. Moreover, it provides for new implications in the involvement of both private and State-owned business in the production and dissemination of this technology across the globe. From Gaza and Ukraine to Sudan and South Asia, the deployment of AI systems illustrates how the intersection of military ambition, private enterprise, and weak legal oversight has reshaped the global security-business nexus. While the scale and sophistication of AI use differ between the aforementioned contexts, the underlying issues of accountability, transparency, and human rights violations remain the same in each and every context.

In Europe and the Middle East, AI has become both an economic and political instrument. Ukraine’s “tech war” demonstrates how a State can mobilise private firms and foreign partners to develop autonomous systems that offset conventional war disadvantages. Yet, this development signposts the erosion of meaningful human control in warfare, with AI systems increasingly substituting human judgement in targeting and combat operations. Similarly, Israel’s use of Lavender, amongst others, illustrates the dangers of AI-driven targeting when deployed without ethical or legal oversight. The result is indiscriminate and disproportionate killing of civilians in Gaza to the degree of genocide. The cost of modernisation

of the defence industry through these systems is felt mostly by civilian populations signifying to us that AI's military utility and potential, without legal and ethical regulations, will supersede humanitarian restraints.

By contrast, conflict in Southeast Asia and Africa reveal a more indirect yet equally troubling pattern where AI systems are utilised for its potential to control, surveil, and suppress masses. In Myanmar, Chinese-supplied AI systems intended for facial recognition and digital tracking have facilitated systematic human rights abuses, but ones revolving around rights to privacy and freedom of expression. A similar development is present in the DRC and Sudan, where Chinese and Turkish made drones and AI systems technology are being deployed on battlefields and in civilian areas by both State and non-State actors. Though the automatised AI technology has not reached levels present in Europe and the Middle East, the use of AI systems in Africa and South Asia increasingly underpin the logistical execution of warfare and societal control. These applications, though less overtly militarised than AI-driven drones or targeting systems, underscore that AI's integration in the defence industry risks extending beyond warfare to encompass State surveillance and digital authoritarianism.

Despite contextual variations, the same major powers, China, Russia, and the United States, dominate the development, supply, and export of AI based military systems. Through State-owned, and State-supported private contractors/companies, each contributes to an expanding global market projected to double in valuation, jumping from around USD 9.3 billion to USD 19.2 billion in the period 2025-2030 (Grand View Research 2024). Companies such as Lockheed Martin and Palantir in the US, CASIC and Danhua in China, as well as Rostec and Kalashnikov Concern in Russia, contribute to this expansive economical underpinning of development and incorporation of AI systems into warfare, increasingly prioritising profit over ethics and long-standing pillars of international law (Losey 2025).

To avoid such violations of IHL, it is first recommended that States engaging with AI systems as part of their military tactics adhere to key principles of transparency, accountability and civilian harm mitigation, remembering that these principles are still applicable to AI and are mandatory for legal warfare (Dorsey and Moffett 2025). Meanwhile, the ICRC (2024, 7–8) specifies that further steps should be taken to establish binding legal frameworks that:

- Restrict AI targeting to lawful military objectives,
- Limit operational scope and duration to ensure human supervision
- Prohibit deployment in civilian areas
- Guarantee real time human control and ability to intervene

When considering responsible AI use and accountability from technology companies, conversations have been ongoing regarding the

prioritisation of “beneficial intelligence” and “value alignment” within AI use through the Asilomar principles (Garcia 2019). Firstly, to ensure that creators of AI systems have a moral responsibility in their design, use, and actions. Secondly, autonomous systems that are developed will share the same values and goals that drive human behaviour. As such, “the design of such systems must be compatible with human dignity, rights, and freedoms” (Garcia 2019, 3). Such value alignment would apply customary law to the decision-making and actions of such systems. Given the use of AI systems by Israel’s military and the observed violations of IHL, it is crucial now more than ever to implement these ideas. The ICRC has issued a stark warning, emphasising that “if algorithms are trained in overly permissive targeting rules, the result will be death and destruction among civilians at greater speed and on a larger scale” (ICRC 2024: 7–8), highlighting the urgent need for careful oversight and strict compliance to protect civilian life.

References

- AAPP. 2025. “List of Arrests Cases and Warrants in Myanmar.” October 17. [Link](#) (last visited 23 July 2026).
- Abdurasulov, A. 2025. “The New AI Arms Race Changing the War in Ukraine.” BBC News. October 10. [Link](#) (last visited 23 July 2026).
- Abraham, Y. 2023. “‘A Mass Assassination Factory’: Inside Israel’s Calculated Bombing of Gaza.” *972 Magazine*. November 30. [Link](#) (last visited 23 July 2026).
- Abraham, Y. 2024. “‘Lavender’: The AI Machine Directing Israel’s Bombing Spree in Gaza.” *972 Magazine*. April 3. [Link](#) (last visited 23 July 2026).
- Africa Defense Forum. 2025. “‘Made in Africa’ drones take off.” *Africa Defense Forum* 17(4), 13. [Link](#) (last visited 23 July 2026).
- African Charter on Human and Peoples’ Rights (adopted 27 June 1981, entered into force 21 October 1986) (1982) 21 ILM 58.
- Allen, N., and I. Okpali. 2022. “Artificial intelligence creeps on to the African Battlefield.” Brookings Techstream Blog. February 2. [Link](#) (last visited 23 July 2026).
- Andersin, E. 2025. “The use of the ‘lavender’ in gaza and the law of targeting: ai-decision support systems and facial recognition technology”. *Journal of International Humanitarian Legal Studies*, 16(2), 336-370.
- Arab News. 2025. “Drone attack strikes Sudan capital: Army source.” October 14. [Link](#) (last visited 23 July 2026).
- ASEAN. 2024a. *ASEAN Guide on AI Governance and Ethics*.
- ASEAN. 2024b. *ASEAN Responsible AI Roadmap (2025-2030)*.
- Austero, Mitzi, and Pauleen Gorospe Savage. n.d. *Artificial Intelligence, Emerging Technology, and Lethal Autonomous Weapons Systems*.
- Aye, N. C. 2024, October 9. “Observers: Chinese-made fighter jets play key role in deadly airstrikes in Myanmar”. *Voice of America*. [Link](#) (last visited 23 July 2026).

- Ayferam, G. 2023. "Sudan's conflict in the shadow of coups and military rule." Carnegie Endowment for International Peace. August 16. [Link](#) (last visited 23 July 2026).
- Bah, A. S. 2024. "Remarks by Dr. Alhaji Sarjoh Bah, Director of Conflict Management Directorate on autonomous weapons system: An ECOWAS perspective." African Union Commission.
- Bergengruen, V. 2024. "Tech Companies Turned Ukraine into an AI War Lab." Time. February 8. [Link](#) (last visited 23 July 2026).
- Boffey, D. 2025. "Killing Machines: How Russia and Ukraine's Race to Perfect Deadly Pilotless Drones Could Harm Us All." The Guardian. June 25. [Link](#) (last visited 23 July 2026).
- Bondar, K. 2024. "Understanding the Military AI Ecosystem of Ukraine." Center for Strategic and International Studies. November 12. [Link](#) (last visited 23 July 2026).
- Books, W. O. 2025. *The Genie Is Out: Is AI a Tool of War or Peace? Sustainable Development Without Borders: Western Sydney University to the World*.
- Bunnag, K. 2022. *Artificial Intelligence Arms Race: Opportunities for ASEAN and Thailand's Defence Capability*. Friedrich Naumann Foundation for Freedom.
- Chambers, J., and N. Cheesman. 2024. "Introduction: Revolution and Solidarity in Myanmar." *Journal of Contemporary Asia* 54 (4): 1–10. [Link](#) (last visited 23 July 2026).
- Cvetković, I. R. 2025. "If machines could speak: What can the AI-powered technologies used in Gaza tell us about Israel's genocidal intent?". *Criminological Encounters*, 7(1).
- De Vynck, G. 2023. "Artificial Intelligence and the War in Ukraine." In *Artificial Intelligence and the War in Ukraine*, edited by J. Pardo de Santayana. Spanish Ministry of Defense. [Link](#) (last visited 23 July 2026).
- Dorsey, J., and L. Moffett. 2025. "The Warification of International Humanitarian Law and the Artifice of Artificial Intelligence in Decision-Support Systems: Restoring Balance through the Legitimacy of Military Operations." SSRN Working Paper No. 5239131. [Link](#) (last visited 23 July 2026).
- European Union. 2024. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Official Journal of the European Union. [Link](#) (last visited 23 July 2026).
- Fazi, T. 2024. "Gaza: The World's First AI-Powered, Robot-Enabled Genocide." Counterfire. March 8. [Link](#) (last visited 23 July 2026).
- Flournoy, M. A. 2023. "AI is Already at War." Foreign Affairs. November 28. [Link](#) (last visited 23 July 2026).
- Garcia, E. 2019. "Artificial Intelligence, Peace and Security: Challenges for International Humanitarian Law." *Cadernos de Política Exterior* 8: 112–30.
- Graceffo, A. 2025. "China's Global Security Initiative and the Burma Junta's PSMS Surveillance". MIZZIMA. [Link](#) (last visited 23 July 2026).
- Grand View Research, Inc. 2024. "Artificial Intelligence in Military Market: Industry Analysis, Market Size, Share & Forecast, 2025–2030." [Link](#) (last visited 23 July 2026).
- Helal, H. 2024. "Common African Position on the Application of International Law to the Use of Information." [Link](#) (last visited 23 July 2026).
- Holland, M. A. 2024. *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision-Making*. International Committee of the Red Cross. [Link](#) (last visited 23 July 2026).

- Hussain, A. 2025. "Pakistan Launches Operation Bunyan Marsoos: What We Know So Far." Al Jazeera, May 10. [Link](#) (last visited 23 July 2026).
- International Covenant on Civil and Political Rights (ICCPR). 1966. UN General Assembly Resolution 2200A (XXI) of 16 December 1966, entered into force 23 March 1976. 999 UNTS 171.
- International Committee of the Red Cross. 1977. *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, Article 48. International Committee of the Red Cross. [Link](#) (last visited 23 July 2026).
- ICRC. 2024. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*. [Link](#) (last visited 23 July 2026).
- Kallenborn, Z. 2021. *InfoSwarms: Drone Swarms and Information Warfare*. Modern War Institute, United States Military Academy. [Link](#) (last visited 23 July 2026).
- Kirichenko, D. 2025. "Artificial Intelligence's Growing Role in Modern Warfare." War Room – U.S. Army War College. August 21. [Link](#) (last visited 23 July 2026).
- Köckritz, Angela. 2025. "Myanmar: AI Helps to Identify Opposition Members." Table.Briefings. December 1. [Link](#) (last visited 23 July 2026).
- Kuele, G. 2015. "Using drones for conflict prevention in peacekeeping operations." Instituto Igarapé. [Link](#) (last visited 23 July 2026).
- Kuzio, T. 2025. "Russia's War Transforms Ukraine into a World-Leading Military Producer." The Jamestown Foundation. October 5. [Link](#) (last visited 23 July 2026).
- Losey, S. 2025. "Drones, AI and Robotics Challenge Order of Top 100 Defense Firms." Defense News. September 2. [Link](#) (last visited 23 July 2026).
- Maksymiv, S. 2025. "Black Mirror #26: Russian Military Innovations." The Defender, September 29. [Link](#) (last visited 23 July 2026).
- Mamedieva, G. 2025. "Military AI: Lessons from Ukraine." Tech Policy Press. March 20. [Link](#) (last visited 23 July 2026).
- Matamis, J. 2025. "Too Little, Too Late: China Steps Up Military Aid to Myanmar's Junta." Stimson Center. March 4. [Link](#) (last visited 23 July 2026).
- Militär Aktuell. 2025. "Chinese Wing Loong II drones for the DR Congo." May 2. [Link](#) (last visited 23 July 2026).
- Ministry of Defence. 2025. "Joint Statement By The Asean Defence Ministers on Cooperation in the Field of Artificial Intelligence in The Defence Sector." February 26. [Link](#) (last visited 23 July 2026).
- Myanmar: "Justice for Myanmar report finds Chinese tech firms allegedly aid junta's digital surveillance and censorship." (n.d.). *Business & Human Rights Resource Centre*. [Link](#) (last visited 23 July 2026).
- Oliinyk, O. 2025. "Legal Regulation of Artificial Intelligence in Ukraine: Challenges and Prospects." *Social Development: Economic and Legal Issues* 6: 32–45. [Link](#) (last visited 23 July 2026).
- Onderco, M. 2025. "Navigating the AI Frontier: Insights from the Ukraine Conflict for NATO's Governance Role in Military AI." *Journal of Strategic Studies* 48 (3): 602–26. [Link](#) (last visited 23 July 2026).
- Pardo de Santayana, J. 2024. *Artificial Intelligence and the War in Ukraine*. Spanish Ministry of Defense. [Link](#) (last visited 23 July 2026).
- Philip, S. A. 2025. "Op Sindoor Is India's First AI-Enabled Operation: How 'Heavy Use' of Modern Tech by Army Played Out." The Print. October 7. [Link](#) (last visited 23 July 2026).

- Potkin, F. 2022. "Exclusive: Myanmar's Junta Rolls Out Chinese Camera Surveillance Systems in More Cities." Reuters. July 11. [Link](#) (last visited 23 July 2026).
- Quantum Systems. 2024. "Quantum Systems Deploys 'Receptor AI' in Ukraine for the First Time." July 12. [Link](#) (last visited 23 July 2026).
- Rahman, Muhammad Faizal Bin Abdul. 2026. "AI in Defence: The Way Forward for ASEAN's ADMM Cooperation." June. [Link](#) (last visited 23 July 2026).
- Rahmtall, Albadawi. "Drones in the Sudanese War." Military Africa. June 18. [Link](#) (last visited 23 July 2026).
- Reuters. 2024. "Around 20 civilians killed in Congo attack, army and rebels trade blame." January 25. [Link](#) (last visited 23 July 2026).
- Sareen, S. 2025. "Algorithmic sovereignty in South Asia: India's use of AI in the 2025 border conflict." *Journal of Military and Strategic Studies* 24 (2) 81-112.
- Serhan, Y. 2024. "How Israel Uses AI in Gaza—and What It Might Mean for the Future of Warfare." Time. December 18. [Link](#) (last visited 23 July 2026).
- Serwat, Ladd. 2025. "Armed Conflict Location & Event Data Project [ACLED]." March 23 Movement (M23). [Link](#) (last visited 23 July 2026).
- Shahzad, S. A. 2024. "Adoption of AI in Warfare: Comparative Study of India and Pakistan." *Journal of Academic Research for Humanities* 7 (3): 112–25.
- Singh, Navdeep. "China Defence Stocks Jump Up to 36% amid India-Pakistan Tensions after Operation Sindoor." The Economic Times, May 8, 2025. [Link](#) (last visited 23 July 2026).
- The Times of India. 2025. "Opposition Briefed on Operation Sindoor, 13 Civilians Killed in Pak Shelling: Key Developments." May 8. [Link](#) (last visited 23 July 2026).
- The News International. 2025. "Shares of Rafale Maker Plunge, China's Defence Stocks Advance as Pakistan Downs IAF Jets." The News International. May 8. [Link](#) (last visited 23 July 2026).
- Thura, A. 2025. "'Made in China': Inside the Myanmar Junta's Intensifying Drone Offensive." The Irrawaddy. March 3. [Link](#) (last visited 23 July 2026).
- Turkish Minute. 2025. "Turkey's Baykar sent \$120 million in drones and missiles to Sudanese Army report." March 8. [Link](#) (last visited 23 July 2026).
- UN General Assembly. 2014. Resolution Adopted by the General Assembly on 18 December 2013 (A/RES/68/167). [Link](#) (last visited 23 July 2026).
- United Nations, General Assembly. 2024. Lethal autonomous weapons systems: report of the Secretary-General. A/79/88. July 1. [Link](#) (last visited 04 August 2026).
- United Nations. 2024. "Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts, Report of the Secretary-General." A/79/224. July 23. United Nations.
- United Nations Human Rights Council. 2025. "Report of the Independent International Fact-Finding Mission for the Sudan." Document A/HRC/60/22. Advance edited version.
- United Nations Human Rights Office of the High Commissioner. "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework. New York and Geneva: United Nations, 2011. [Link](#) (last visited 04 August 2026).
- United Nations Working Group on Business and Human Rights. 2022. "Responsible business conduct in the arms sector: An information note." [Link](#) (last visited 23 July 2026).

- United Nations. 1980. *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects* (Convention on Certain Conventional Weapons). United Nations. [Link](#) (last visited 23 July 2026).
- Verbrugge, B., D. Verbruggen, and H. Merket. 2025. "Human rights due diligence in the global defence industry: Lessons from other sectors." [Link](#) (last visited 23 July 2026).