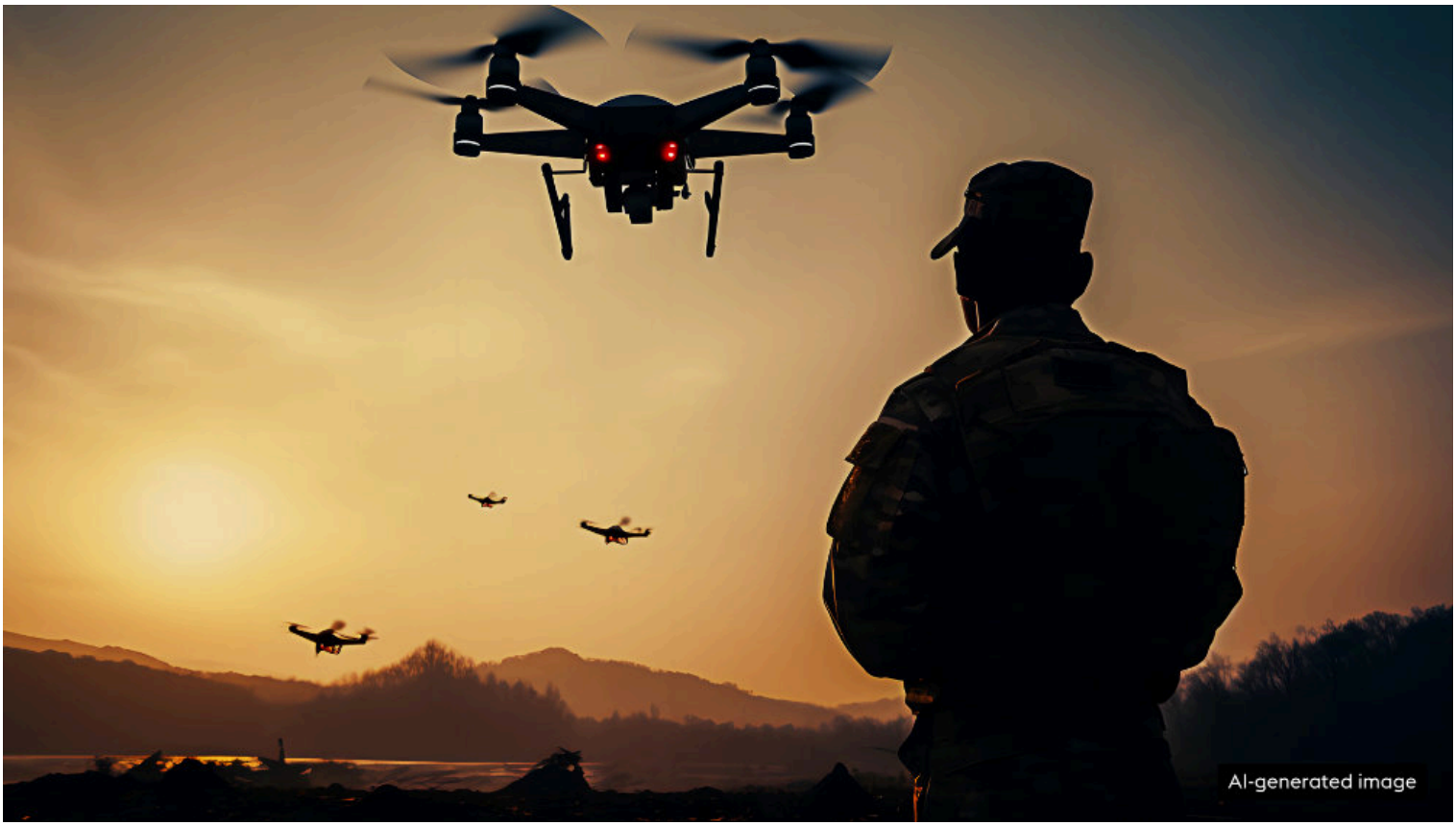
HUMANITARIAN
LAW & POLICY

The shifting battlefield: technology, tactics, and the risk of blurring lines of warfare

May 22, 2025, Analysis / Conduct of Hostilities / Humanitarian Principles / IHL / Law and Conflict / New Technologies / Weapons

12 mins read

Ruben Stewart
ICRC Adviser on Technology in Warfare



The accelerating integration of emerging technologies into armed conflict is transforming not only the tools of war, but its tactics, geography, participants and impact. Technological developments — from commercial drones to artificial intelligence, electronic warfare to the military use of civilian infrastructure — risk undermining boundaries between military and civilian domains. These changes challenge long-held assumptions about the character and conduct of warfare, how wars are fought in practice, while raising legal and humanitarian concerns for the protection of civilians and the preservation of the principle of distinction.

In this post, Ruben Stewart, ICRC Adviser on New Technologies of Warfare, explores the drivers and implications of this transformation. He focuses on how evolving technologies and trends are influencing the conduct of hostilities and impacting the protection of civilians. He underscores the urgent need to uphold legal norms amid these shifts, particularly the principle of distinction, ensuring that complexity does not become a pretext for non-compliance. At the heart of his analysis is a call to reckon with the profound humanitarian consequences these changes impose on those caught in conflict.

ICRC Humanitarian Law & Policy Blog · The shifting battlefield: technology, tactics, and the risk of blurring lines of warfare

The *character of armed conflict* is changing. Innovations once confined to the science fiction genre or laboratories are deployed on today's battlefields. At the same time, new methods of warfare are emerging that risk blurring long-standing lines: between military and civilian, physical and digital, and activities that are part of an armed conflict and those that aren't. This transformation is not merely technological; it is conceptual, doctrinal, and strategic.

Conflict today is shaped by three overarching and interconnected trends: the pursuit of *reduced risk* driven by force protection considerations, the drive to *increase lethality*, and the growing *integration of civilians and civilian objects into military activities*. Each poses distinctive challenges to the protection of civilian populations, the application of international humanitarian law (IHL), and risks shaking some of the very assumptions that underlie the conduct of war.

The rise of uncrewed and autonomous systems

Arguably the most visible and widely adopted military innovation of the last decade has been the proliferation of uncrewed systems: drones in the air, vehicles on the ground, and vessels at sea. Once accessible *only to a handful of technologically advanced states*, they are now a near-ubiquitous feature of contemporary warfare, including by non-state armed groups (NSAG).

Two categories dominate this landscape. First are *commercial-off-the-shelf (COTS) systems repurposed for military use* that are affordable, adaptable, and often disposable. Originally designed and built for civilian use they are now used for *Intelligence, Surveillance and Reconnaissance (ISR), Command and Control and Communications (C3)* and, increasingly, to *undertake attacks*. Second are purpose-built uncrewed systems designed specifically for military operations. These include long-range strike drones, autonomous loitering munitions, and ground-based platforms for *combat support*, *logistics*, and even *medical evacuation*.

Production figures from ongoing conflicts demonstrate the scale of this transformation. Where once only a few states had access to a limited number of systems, the majority of state militaries now have access to fleets of systems, some *numbering in the millions*. These numbers indicate not just *tactical adaptation but a fundamental shift* in how military force is generated and projected.

Uncrewed maritime and ground vehicles are also rapidly advancing. Naval drones have been used in offensive operations against *ships*, *coastal targets*, *helicopters and fixed wing aircraft*. Ground platforms are being trialled and deployed for everything from *mine-laying* to *combat support*. A *recent joint operation conducted entirely by uncrewed systems*, albeit at limited scale, offers a glimpse of what fully automated conflict might one day entail.

Seeing everything, everywhere, all the time: persistent sensors and the information environment

Another defining feature of today's battlefield is the explosion in data collection and sensor integration. Modern militaries and non-state actors rely on a vast array of inputs such as *thermal imaging and night vision devices*, Light Detection and Ranging (*LiDAR*), radar, *acoustic sensors*, metadata, and *satellite feeds* to create a common operational picture (COP).

But this COP is not generated by military assets alone. *Civilian devices, especially mobile phones, serve as both intelligence gathering and command, control and communication systems*. Phone users can knowingly collect and transmit battlefield intelligence but in other instances, *their devices are used without their knowledge to locate, track, and categorize them for potential targeting*. Vast amounts of *personal data, such as call logs, app metadata, and geolocations can be harvested from civilian sources, processed by AI-enabled systems,* and repurposed for targeting, profiling, or influence operations.

To facilitate the transfer and processing of this information, there has also been a merging of civilian and military information infrastructure and tools. *Commercial satellites*, *data centres, civilian software* and telecommunications networks are now routinely used to *translate*, *categorize and store communications* intercepted by the military, *transmit battlefield data*, and *facilitate command and control*.

The legal implications are stark. When *civilian digital infrastructure becomes instrumental to military operations*, it may also become a military objective. In addition, *individuals risk being targeted not for what they do, but for what their devices appear to reveal about them*.

The invisible battlefield: electronic warfare and communication interference

As reliance on digital communication has grown, so too has the vulnerability of these systems. Electronic Warfare (EW), including jamming, spoofing, and signal interception has become *a central component of contemporary conflict*.

In some engagements, EW has reduced the accuracy of precision-guided munitions from a *margin of error of under 20 metres to more than a kilometre*. Crewed and uncrewed aerial systems have been grounded, *forced to abort their flights*, or *lost due to jamming*. Encrypted radios have been captured or rendered useless, forcing operators to revert to analogue tools such as *paper maps and using commercial mobile phones*.

Commercially available *jammers are now in use by non-state actors* to disrupt communication and navigation. In addition to their tactical effects, electronic emissions themselves create risks: even brief emissions can reveal *a unit's location* for targeting.

In response, some militaries are adopting more resilient systems, such as *fibre-optic communication lines for drones*. Others are experimenting with *autonomous weapons* that do not require an active control link at all, effectively removing humans from a decision-making role.

Artificial intelligence and the speed of war

Artificial intelligence (AI) is rapidly becoming a tool in how wars are fought. AI is being used to *identify targets*, analyze and manage sensor data, translate communications, and *plan and coordinate uncrewed operations*. In conflict, AI-enabled systems can compress the "kill chain" (the sequence from detection to strike) *from minutes to seconds*. In some applications, AI has reportedly been used to *recommend targets* and even facilitate strikes with apparently limited human review.

Current AI systems are generally designed to support, rather than replace, human decision-making. But this support can become substitution when decisions are made at such speed that human oversight is functionally impossible — a condition sometimes described as "*AI singularity*".

Beyond targeting, *AI is being integrated into logistics, surveillance, and strategic planning*. Militaries are pursuing "human–machine teaming" concepts, pairing AI powered platforms with crewed systems to enhance operational efficiency. *Aerial "loyal wingman" systems* – uncrewed aircraft that fly alongside piloted jets – are *already operational in some contexts*.

As AI systems mature, their influence will likely extend across all levels of warfare. At the same time, questions remain about *legal accountability, error rates, and the ability to meaningfully apply IHL* to systems that adapt in ways not even their designers may fully understand.

The increasing use of long-range strike and hypersonic weapons

Another notable trend is the expanded use of long-range and high-velocity weapons, including *extended range drones*, *ballistic missiles*, *cruise missiles*, and increasingly, *hypersonic glide vehicles*. These systems allow actors to strike targets *over 1,000 kilometres away* – far from the front lines and often *deep within the opponent's territory*.

These long-range capabilities have been generated by *developing new systems* and in other cases by *retrofitting existing munitions with enhancements* that extend their range and *converting existing systems such as air-defence missiles to be used in a ground-attack role*.

Hypersonic weapons – defined as those travelling at more than five times the speed of sound – are particularly concerning due to their manoeuvrability and speed, which *render many existing missile defences ineffective*. *Trials* and *deployments* are increasing, with some of the *first operational uses reported in 2024*.

The implications for civilian safety are clear: as the range and speed of weapons increase, so does the *vulnerability of critical infrastructure and population centres* far from frontlines, and often without the mitigation of timely warnings or effective interception by air defence systems.

The expanding domain of warfare

Modern warfare is no longer confined to land, sea, and air – there is *increasing military activity in the cyber and space domains, as well as in the information environment*.

Cyber operations targeting *public infrastructure*, *communications networks*, and *transportation systems* have become more frequent. *Activities below the threshold of armed conflict* such as *GPS interference affecting civilian aviation*, *cyber sabotage*, and *disinformation campaigns* are now routine features of interstate competition.

In space, the sheer number of satellites launched in recent years, *often numbering in the hundreds in a single year*, illustrate the growing centrality of space for ISR and C3. The *jamming, spoofing, or even physical interference* of both military and commercial satellites and concerns about the use of *nuclear-generated electromagnetic pulses (EMP) to disable low Earth orbit satellites* underscore the fragility of this domain.

From defence to "total defence"

In response to the growing scale and complexity of threats, several states have adopted *"total defence" strategies*, i.e. *whole-of-society approaches that integrate military, civilian, economic, and technological resources into national security planning*. These strategies often include *guidance for civilians on how to prepare for emergencies*, *maintain essential services*, and, in some cases, *contribute to national defence efforts*. Additionally, national defence frameworks include considerations of how tech companies and civilian critical infrastructure such as telecommunications, ICT services, and satellite networks may be used to support military defence efforts.

While civilian involvement may enhance states' resilience, involving civilians more directly in support roles – such as *information gathering*, logistics, or *civil resistance* – raises serious humanitarian concerns. For instance, the closer *civilians* and *civilian* ICT *infrastructure* are drawn into military activities, *the greater the risk of exposure to harm and the more challenging respect for the principle of distinction under international humanitarian law*.

States implementing total defence models should consider how to balance preparedness with protection, ensuring that civilians remain safeguarded from the effects of hostilities and are not placed at unnecessary risk through their involvement in military operations.

Humanitarian consequences and the need for reflection

Across all these developments, one worrying trend is constant: the increasing blurring of civilian and military domains. Whether through *the military use of COTS technologies*, *the use of civilian infrastructure for military purposes*, or the *mobilization of civilians* themselves, the line between combatant and non-combatant risks becoming ever more difficult to draw.

This is particularly relevant where the military use of civilians or civilian objects raises questions about the compatibility of such use with the obligation to protect them from the effects of hostilities under IHL. If the line between civilians and the military becomes blurred, the principle of distinction, the obligation to differentiate between military objectives and civilian persons and objects, becomes harder to implement. So too are rules relating to proportionality, precautions in attack, and *the protection of civilian infrastructure*.

Moreover, as warfare becomes *faster, more automated, and more data-driven, the scope for meaningful human judgement narrows*. Decisions with life-or-death consequences may be made at machine speed and based on inputs and programming that are invisible to human operators.

Conclusion: towards a more complex battlespace

The battlespace of the future will be shaped by three converging trends: the *reduction of risk* through uncrewed and long-range systems and automation of dangerous tasks; the pursuit of greater *lethality* through networks of sensors, faster decision making, and multi-domain operations; and we risk seeing a growing *military integration of civilians and civilian objects*, from infrastructure and COTS tools, through to total defence strategies.

These innovations and their employment must be matched by greater consideration of the consequences and adoption of safeguards to reduce the risk of civilian harm. As the character of conflict evolves, armed actors must constantly refer back to legal, ethical, and humanitarian frameworks guiding their application. Technology can reshape how wars are fought, but their causes and whom they affect remain relatively constant.

As the lines blur and warfare accelerates, it becomes ever more urgent to hold firm to the principles and rules that distinguish armed conflict from indiscriminate violence, namely international humanitarian law. These norms are not optional – they are essential to preserving our shared humanity. Far from being a burden, those norms offer a framework to navigate complexity, impose clarity amid confusion, and help ensure that technological innovation does not come at the expense of civilian lives.

See also:

- Ruben Stewart, *From "total war" to "total defence": tracing the origins of civilian involvement in armed conflict*, April 30, 2025

- Joanna Wilson, *AI, war and (in)humanity: the role of human emotions in military decision-making*, February 20, 2025
- Joelle Rizk, *Why is the ICRC concerned by 'harmful information' in war?*, September 10, 2024.
- Ingvild Bode and Ishmael Bhila, *The problem of algorithmic bias in AI-based military decision support systems*, September 3, 2024.
- Wen Zhou and Anna Rosalie Greipl, *Artificial intelligence in military decision-making: supporting humans, not replacing them*, August August 29, 2024.

Tags: armed conflict, Artificial Intelligence, Autonomous Weapons, AWS, Civilians, compliance, conduct of hostilities, Geneva Conventions, IHL, international humanitarian law, modern warfare

You may also be interested in:

Complying with IHL in large-scale conflicts: detention operations in international armed conflicts

17 mins read

Analysis / Conduct of Hostilities / Humanitarian Principles / IHL / Law and Conflict / New Technologies / Weapons

Sylvain Vité & Isabelle Gallino

Large-scale detention operations in international armed conflicts (IACs) pose significant humanitarian, legal, and operational challenges. ...

From "total war" to "total defence": tracing the origins of civilian involvement in armed conflict

14 mins read

Analysis / Conduct of Hostilities / Humanitarian Principles / IHL / Law and Conflict / New Technologies / Weapons

Ruben Stewart

When states adapt "total defence" strategies that mobilize entire populations in preparation for armed conflict, ...