# Ceasefires: Integrating Emerging Technologies

Emerging technologies are changing the nature of warfare. Ceasefire agreements need to respond to the type of violence they seek to address, thus also to the impact of emerging technologies. Adaptations are needed during the preparation, negotiation, and implementation of ceasefires.

By Simon J. A. Mason,
Ivan Zaccagnini,
and Julian Th. Hottinger

The proliferation of emerging technologies including drones, AI, hypersonic missiles, advanced communication networks, cyber, and space-based assets, is increasingly shaping contemporary conflicts. While war still vastly remains a matter of humans, steel, and powder, the diffusion of these technologies affects the battlefield at the tactical, operational, and strategic levels, compelling states and armed forces to adapt. Importantly, this adaptation extends beyond battlefield practices to encompass industrial and organizational dimensions, influencing the development, production, integration, and employment of military systems.

A drone with an attached portable grenade launcher during a test fly conducted by Ukrainian servicemen in the Zaporizhzhia region in Ukraine on 11 October 2024. *Stringer / Reuters*

Different facets of how such emerging technologies are impacting warfare have been observed in various conflicts over the last decade, including in Colombia, Nagorno-Karabakh, Israel-Gaza, USA/Israel-Iran, Yemen-Saudi Arabia, Myanmar, Sudan, and Ukraine-Russia. To various degrees, emerging technologies have shaped battlefield dynamics in all these conflicts and enabled both state and non-state actors to strike faster, deeper, and across new domains. A common pattern across these conflicts is that the interaction of emerging technologies with conventional warfare is where major shifts in fighting dynamics take place, rather than any single technology making the difference.

Emerging technologies are also changing approaches to regulating and stopping violence, such as through ceasefires. This calls for new ways to regulate them in a ceasefire, as well as use them for ceasefire monitoring and verification. Modern ceasefires increasingly need provisions for monitoring uncrewed systems, preventing cyberattacks on civilian infrastructure, and using satellite, sensor, and AI tools to verify compliance and maintain trust between parties. Therefore, ceasefire experts and policymakers must consider the potential benefits, as well as the technical limitations, vulnerabilities, and potential misuse of these technologies when developing balanced and resilient ceasefire agreements and compliance strategies.

This analysis focuses on the methodological dimensions of ceasefires. It is important, however, to see them as embedded in

a specific political reality. Thus far, research has mainly focused on the role of technologies in ceasefires with respect to monitoring during the implementation phase (e.g., studies by Hug, CSS, UNIDIR, Rand, Sticher & Verjee and GCSP). Currently, there is insufficient emphasis on integrating emerging technologies in the preparation and negotiation phases of ceasefires, hence a focus on these and particularly the former in this analysis. Russia's 2022 full-scale invasion of Ukraine provides the most up-to-date insights into how emerging technologies are shaping war today. Lessons drawn regarding the possible implications for ceasefire preparation rely on insights of how emerging technologies are shaping the Russia-Ukraine war, but they also extend beyond this case, demonstrating their potential relevance for other conflicts.

## Ceasefires: Politics and Method

A ceasefire agreement is an agreement between two or more parties in a conflict on how to stop fighting. There is a political and methodological side to ceasefires. The political side is beyond the reach of ceasefire experts, shaped by the decision-makers in the main conflict, who decide on the conditions for a ceasefire and the links between a ceasefire and political negotiations. The purpose of political negotiations is to address the underlying points of disagreement to resolve the conflict and move towards a peace agreement. Within such political parameters, ceasefire agreements have a narrower purpose: to regulate or stop violence. Their purpose is *not* to resolve the conflict, but rather to open the space for political negotiations by addressing conflict violence in a preliminary ceasefire, and then to dismantle the status of war in a definitive ceasefire.

The task of ceasefire experts is to design the "optimum" ceasefire agreement from a methodological perspective. Such a ceasefire agreement will not stop parties from resuming fighting if they want to. However, designing a methodologically sound ceasefire should prevent the ceasefire from collapsing due to ambiguities, lack of detail, and misunderstandings. Ceasefires that do not address emerging technologies are less likely to be effective and sustainable.

## Phases of the Russia-Ukraine War

Russia's ongoing full-scale invasion of Ukraine, which began in February 2022, illustrates how emerging technologies are shaping the nature of warfare. From 2022 to early 2026, the Russia-Ukraine war unfolded in four distinct phases based on the different types of technologies used. A ceasefire agreement built at the end of phase one would have looked markedly different to one built at the end of phases two, three, or four. Depending on the level of technology available to the main actors, future wars may begin by already involving the types of technology that are used in the context of Russia-Ukraine in early 2026 (phase 4), while others may evolve more similarly through the different phases of technology introduction and use. Adaptations of ceasefire drafts from phase to phase are likely to be stacked. Consequently, challenges resulting from a first phase will persist and be compounded by challenges arising from the following phases. Ceasefire drafts may therefore need to respond to different waves of emerging technology as illustrated in the context of the Russia-Ukraine war, cognizant that the evolution of each case and the ensuing response from a ceasefire perspective, will be highly case-specific.

> Emerging technologies are also changing approaches to regulating and stopping violence, such as through ceasefires.

*First phase–February 2022 to summer 2022*: Elements of conventional warfare coexisted with the early impact of military-grade drones and advanced intelligence, surveillance, and reconnaissance (ISR) platforms. Russia initially attempted a rapid, shock and awe operation aimed at capturing Kyiv within days, relying on infantry, paratroopers, armored vehicles, tanks, and logistics columns, with limited use of aviation due to effective Ukrainian air defenses. Ukraine, by contrast, made extensive use of military drones such as the Medium-Altitude-Long-Endurance (MALE) Bayraktar TB2, alongside ISR capabilities largely provided by the US and other Western partners. The combination of sensors and drones enabled Ukrainian forces to track Russian movements, conduct precision strikes, and redeploy troops enhancing urban defense through the effective employment of mobile radars, and man-portable anti-tank (MANPATS) and air-defense systems (MANPADS). Between spring and summer, Moscow announced that it had successfully deployed for the first time a hypersonic missile against targets in western Ukraine, while Kyiv began to rely on naval drones for ISR operations and direct strikes in the Black Sea.

*Second phase–Summer 2022 to early 2023:* The conflict transitioned into a war of attrition. The frontlines largely stabilized, with limited territorial advances and heavy losses of personnel and materiel. Trench warfare and artillery became central to the conflict, while long-range precision systems, such as the High Mobility Artillery Rocket System (HIMARS), gained importance. Space-based ISR and communication assets proved critical, with private actors stepping in. For example, SpaceX, enabled Ukraine to maintain resilient internet and communication networks through the Starlink satellite constellation, even as large portions of its national infrastructure were damaged or destroyed. Ukraine also experimented with anti-drone weapons and indigenous AI-based ISR and decision-support tools, which were previously only used for tracking Russian convoys. Platforms such as Delta have been used more consistently only after August 2022. At the same time, loitering munitions proliferated, particularly on the Russian side, which made extensive use of Iranian-supplied Shahed-136 systems.

*Third phase–Early 2023 to early 2024*: The battlefield saw the persistence of earlier dynamics but with significant introductions. Since late 2022, Russia has significantly strengthened its air defense and electronic warfare posture by redeploying systems from Syria. This has made air operations increasingly costly for Ukraine. Simultaneously, both sides began to experience critical ammunition shortages. Since early 2023, these constraints have pushed Ukraine toward smaller, cheaper, and more expendable drones that can be produced quickly domestically or procured off-the-shelf from international markets. In the same period, Kyiv authorized the adoption of cloud-based data storage. Following this decision, Delta was officially introduced to the Defense Forces and transitioned to a decentralized architecture that relies on extraterritorial cloud hosting to safeguard data integrity against persistent and intensified kinetic and cyberattacks.

*Fourth phase–Early 2024 to early 2026*: The conflict reached its highest level of technological complexity, marked by the coexistence of different legacy and emerging platforms, as well as the wider exploitation of the cyber and space domains. The

 

battlefield was saturated with hundreds of commercial and military drone models, including interceptors, first-person-view and fiber-optic-cabled variants. Both sides used these uncrewed systems in dense electronic warfare environments. Dependence on private companies for drone components, cloud, and satellite services deepened. Meanwhile, AI assumed an increasingly central role in enabling autonomous functions to counter enemy jamming, supporting automatic target recognition and target selection, and enhancing decision-making processes.

Throughout all the above-mentioned phases, various instruments of hybrid warfare – including disinformation campaigns, cyberattacks, and other forms of non-kinetic influence – have been widely and consistently employed by both sides, though predominantly by Russia. This has a major impact on the ceasefire preparation, negotiation, and implementation phases, as well as on how far such activities are mentioned and/or regulated in a ceasefire agreement.

## During Preparations

During the preparation of a ceasefire, as war is ongoing, experts need to follow the evolving nature of warfare and adapt emerging ceasefires drafts to the current phase in a built-up manner. Using the four phases outlined in the context of the Russia-Ukraine war, the following paragraphs explore how a ceasefire would be adapted as the conflict evolved.

When drafting a ceasefire in response to first-phase technologies, the initial preparation step would address conventional elements and military drones. This would include specifying no-fly zones and the latitudes and altitudes at which drones must fly, while maintaining oversight and control of what they might transport. Monitoring hypersonic missiles would require an agreement on joint data sharing and crisis hotlines to allow for rapid detection, attribution and trajectory tracking, with the intention of preventing unintended escalation due to miscalculation.

In response to second-phase technologies, a second step would be taken, building on the first. The wider use of loitering munitions would be addressed, and efforts would be undertaken to understand the increasingly important role of private actors (e.g., Microsoft, Starlink, Amazon, Palantir, and private hackers as part of an IT army), and their relationship with all parties. A ceasefire may, for example, outline the new roles and responsibilities of private business actors during both the preparation and implementation stages. It could also specify that the main conflict parties are responsible for managing the private hacktivist groups they encouraged during the conflict.

In responding to third-phase technologies, a third step could outline options for joint oversight of large and small drone operations. These could include establishing a shared monitoring system and safety protocols to foster cooperation and mutual security. In particular, improving drone traffic and mission-compliance functions would be key. This would involve registering drones, reporting incidents, establishing safe zones, and monitoring compliance with parameters such as mission purpose, airspace, geofences, altitude, routes, aircraft limits, weather minimums, command-and-control standards, safety distances, regulatory permissions, and all other data security requirements.

In responding to fourth-phase technologies, a fourth preparation step would be to draft an agreement requiring military forces and technologies to operate effectively in highly contested and disrupted environments from the outset of a ceasefire. This would entail building communication systems with backup channels in case primary links are jammed, developing navigation tools that do not solely rely on Global Navigation Satellite System (GNSS), enabling specific systems to operate autonomously if contact with operators is lost, and strengthening defenses against cyber threats, such as network sniffing and spoofing. It would also require frequent software and tactical updates, as well as training personnel under conditions that realistically simulate degraded or denied communications and digital systems.

> Integrating emerging technologies into ceasefires requires a change in how ceasefires are defined, built, and negotiated.

## During Negotiations

To date, emerging technology has been mentioned in some recent ceasefire agreements, albeit with few details. Yet, emerging technologies are not merely side issues; ceasefire clauses must redefine what needs to be regulated, as well as how to maintain or restore compliance if it is broken. While the technical protocols to regulate such technologies are important, thoughts must also be given to where and how these clauses are integrated into the ceasefire agreement text. This ensures overall coherence and implementability. Therefore, they should appear as a standalone chapter after the section on core ceasefire mechanics and before the section on monitoring and verification. Placed there, the chapter bridges traditional rules and verification by clarifying how drones, AI, cyber, electronic, and space-based systems are regulated, which uses are permitted, and how control, attribution, and automation affect compliance.

During ceasefire negotiations, a question arises: Should all emerging technologies be addressed in a ceasefire agreement, or only those that can be clearly regulated? This is particularly relevant for cyber operations, which typically fall into a grey zone of neither war nor peace and may be part of routine intelligence gathering. One approach is to include any topic discussed and negotiated between the parties in the ceasefire agreement, even if they cannot all be regulated and monitored. This would prevent parties from claiming that they were unaware of the dynamics. At the same time, it

### Expertise on the Topic

**States** with ceasefire mediation expertise on this topic include Switzerland and Norway, who deploy experts to conflicts. They also co-organize the annual UN Ceasefire Mediation Course with the UN. States working on the needs of drones for military and defense purposes and for ceasefire monitoring include the USA, the UK and various EU member states.

**International organizations** with expertise used in conflicts around the world include the UN Mediation Support Unit and standby team, and ceasefire monitoring expertise of the OSCE.

**Non-state mediation support actors** working on ceasefires include the CSS and Center for Humanitarian Dialogue (HD), which have a joint project on Ceasefire Mediation funded by the European Union. Combining such know-how with expertise on emerging technologies, e.g. as found at ETH Zurich and with other actors of the Swiss tech eco-system, can bring comparative advantages together to help adapt ceasefire to current developments.

is also important to clearly specify what will be monitored and verified, to avoid misunderstandings and false accusations that the ceasefire is being violated. This will also provide monitoring actors (e.g., states, UN, OSCE) with a clear mandate.

On a policy level, integrating emerging technologies into ceasefires requires a change in how ceasefires are defined, built, and negotiated. Traditional ceasefire agreements focus on halting physical hostilities, but they often fail to address cyberattacks, drone operations, AI-enabled targeting, or digital disinformation campaigns. This creates loopholes that allow parties to claim compliance while continuing harmful non-kinetic actions. Therefore, when drafting such an agreement, policymakers must broaden the case-specific definition of ceasefire to explicitly include cyber and technological operations. They must also establish clear standards for what constitutes a violation and tackle the legal gaps surrounding autonomous systems and AI-driven decision-making. The growing role of private technology companies also needs to be addressed, as they control many of the tools used in modern conflicts, including satellite imagery and communications, cloud platforms, and social media. They also play an increasingly important role in procuring and resupplying components and commercially available off-the-shelf platforms. To prevent technological escalation during the ceasefire, ceasefire agreements may need provisions governing corporate neutrality, the protection of civilian digital infrastructure, data sharing, dual-use export controls, and platform moderation.

Emerging technologies can support implementation by expanding the geographic scope and duration of monitoring and reducing costs.

## During Implementation

The question of which emerging technologies require monitoring during ceasefire implementation needs to be considered separately from how emerging technologies can be used for such monitoring tasks.

Emerging technologies make violations harder to detect and attribute, especially in cyber operations or when small drones and AI-generated content are involved. This requires new monitoring frameworks that combine satellite imagery, cyber forensics, drone detection, and open-source intelligence. To consider technological developments that may occur during implementation, ceasefire agreements need built-in elasticity, ensuring that they periodically review the impact of new or evolving technologies in the ceasefire.

Emerging technologies can support implementation by expanding the geographic scope and duration of monitoring and reducing costs. However, they are likely to complement rather than replace human monitors. Technology can build trust through shared monitoring systems, real-time surveillance of violations, and impartial digital oversight mechanisms. Functionally, emerging technologies in monitoring can be divided between data collection systems, such as satellites and drones, and analytical support systems, such as AI, that process data to detect patterns, identify anomalies, and support verification. They can expand coverage of inaccessible areas and automate the detection of potential violations. Early examples were seen in Colombia's 2016 ceasefire with FARC. Satellite imagery, GPS tracking, and digital registration tools were used to monitor disarmament and remote cantonment zones, which supported verification and trust-building. This was especially effective in tracking sites and actors in geographically remote locations throughout the country.

However, such tools also pose risks: algorithmic opacity, data bias, overreliance, system failure, and technical vulnerabilities may undermine reliability and accountability, while perceptions of intrusive or asymmetric surveillance can erode trust among parties. Therefore, their effectiveness depends on robust human oversight, clear governance frameworks, and agreed-upon verification protocols, which require policy adaptations. Policymakers need to develop accepted attribution standards and dispute-resolution mechanisms, particularly for incidents involving autonomous or semi-autonomous systems.

To manage these opportunities and risks, the international community will need adapted policy frameworks, greater collaboration between ceasefire and technology expert communities, and technology-inclusive ceasefire protocols to prevent accidental escalation, e.g. caused by automated or remote systems.

**For more on perspectives on mediation and peace promotion, see CSS core theme page.**

This analysis is based on research carried out as part of the Ceasefire Mediation Project, a collaboration between the CSS and HD, funded by the EU. The views expressed in this publication are those of the authors, and not necessarily those of the publishing or donor institutions.

**Simon J. A. Mason** is the Head of the Mediation and Peace Team at the Center for Security Studies (CSS) at ETH Zürich.

**Ivan Zaccagnini** is a Researcher in the Global Security Team at the CSS.

**Julian Th. Hottinger** is a retired Senior Mediator at the Swiss Federal Department of Foreign Affairs and a ceasefire expert.

**CSS Analyses in Security Policy** is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Névine Schepers
Language editing: Lisa Fischer
Layout and graphics: Miriam Dahinden-Ganzoni, Rosa Guggenheim

Feedback and comments: css.info@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses




ISSN: 2296-0244; DOI: 10.3929/ethz-c-000797089