GCSP
Geneva Centre for Security Policy

Enabling Peace:

The Potential Use of Technology for Ceasefire Monitoring in Ukraine

JANUARY 2026

Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security and peace. The foundation is supported by the Swiss government and governed by 55 member states. The GCSP provides a unique 360° approach to learn about and solve global challenges. The foundation's mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions to build a more peaceful future.

Authored by **Dr Walter Kemp** under the direction of **Ambassador Thomas Greminger**
Infographics by Chantal Beck

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-038-9

Executive summary

- The size of the territory that may have to be monitored as part of a ceasefire in Ukraine could be massive, including a more than 1,000-kilometre front line.
- Technology can be a key enabler of ceasefire monitoring by producing a clearer, more accurate and comprehensive picture of what is going on.
- A multi-layered approach should be used on land, in the air and at sea, drawing on a range of technological options.
- The effective use of technology can reduce the number of human monitors needed for ceasefire monitoring and increase both the range of possible monitoring and the accuracy of related information.
- Technology should be regarded as a complement to human monitors, not a replacement for them.
- Using technology to strengthen compliance is only credible if there is a mechanism to follow up on any violations of the ceasefire.
- The use of technology for ceasefire monitoring in Ukraine could generate a vast amount of information. The management and security of this information will be crucial and will require an integrated information management system that involves and is trusted by the conflict parties.
- Third parties may be necessary to deploy and operate technology for ceasefire monitoring and for analysing and managing the information gathered by it. The type of technological assets that can be used for monitoring will play a vital role in determining the composition of an international mission. For example, in addition to civilian monitors, it may be necessary to deploy military units and/or private contractors who have the necessary skills and equipment.
- What is technically possible is not always politically possible. The use of technology for ceasefire monitoring will require the consent of the parties and agreed modalities. The use of technology by third-party monitors will have to be spelled out in detail.
- Experience shows that technology used for ceasefire monitoring may be targeted by the parties. The risk of such violations should be mitigated through agreed rules of engagement and agreed procedures for regulating the use of UAVs over a buffer zone.
- Since Russia and Ukraine have been engaged in cyber warfare, a ceasefire should include steps to reduce cyber attacks.

Contents

Introduction

Technology has played a key role in the war between Russia and Ukraine. It can also play an important role in bringing peace. For any agreement to stick, there will have to be a degree of confidence from both sides that a ceasefire is not being violated. This will require monitoring and, if possible, verification coupled with an accountability mechanism.

The difference between monitoring and verification

In the context of a ceasefire, *monitoring* refers broadly to observing compliance with an agreement using visual or technical means, as well as the gathering of information on site or remotely from various sources.

Ceasefire *verification* usually refers to an assessment of a conflict party's compliance with specific provisions of an agreement. This usually involves checking whether certain agreed tasks have been carried out, such as the redeployment of forces or heavy weapons, or following up on incidents.[1]

The size of the territory that will need to be monitored is so vast – most likely a line of contact of over 1,000 km with a buffer zone 15 km wide, as well as depth areas behind the front lines – that it would be difficult to mobilise the necessary number of monitors. Furthermore, some of the territory where monitoring and verification would take place is heavily mined or difficult to access. An additional consideration is that monitoring will not only be necessary on land, but also in the air and at sea.

This paper looks at the possible role of technology in ceasefire monitoring and verification in Ukraine. It is intended and designed to supplement the ceasefire toolkit developed by the GCSP in February 2025.[2] It draws on Alexander Hug's monograph on lessons learned from the use of technology for ceasefire monitoring and verification during the deployment of the OSCE Special Monitoring Mission (SMM) to Ukraine between 2014 and 2021[3] and a Rand Corporation research report on best practices, lessons learned, and the role of technology in designing a ceasefire.[4] The paper also benefited from interviews and feedback provided by experts.[5] The objective of the paper is to provide policymakers and practitioners with options for how technology can help to achieve a sustainable ceasefire in

1 See UN DPPA (United Nations Department of Political and Peacebuilding Affairs) (2022) *Guidance on Mediation of Ceasefires*, https://peacemaker.un.org/sites/default/files/document/files/2022/11/ceasefire-guidance-2022-0.pdf.

2 GCSP (Geneva Centre for Security Policy) (2025) "Drawing a Line: A 'Swiss Army Knife' of Options for Achieving a Ceasefire in Ukraine", February, https://www.gcsp.ch/sites/default/files/2025-03/GCSP_CF-Toolkit_2025%3Bdigital.pdf.

3 A. Hug (2024) *Ceasefire Monitoring and Verification and the Use of Technology: Insights from Ukraine 2014-2022*, Zurich, Center for Security Studies (CSS), ETH Zurich.

4 S. Charap et al. (2025) *Guidelines for Designing a Ceasefire in the Russia-Ukraine War*, Santa Monica, RAND Corporation.

5 The author would like to thank, among others, Valerie Sticher, Vladimir Petchkovsky, Sarah-Marie Grand-Clement, Benjamin Cook, Kjølv Egeland and the GCSP's network of ceasefire experts.

Ukraine and to put the use of technology into context in relation to other factors that are crucial for successful ceasefire monitoring.

A consideration throughout this report is that technology can be a key enabler for monitoring a ceasefire in Ukraine, but it is up to the parties to the conflict to ensure that a ceasefire holds. If technology is to be used for ceasefire monitoring, third parties will be needed to operate the technology and use the data that it generates. This increases the need for international ceasefire monitors.

Added value of using technology for ceasefire monitoring

Technology is not a panacea for foolproof ceasefire monitoring, nor is it a replacement for human monitors. However, it can significantly improve the efficiency, accuracy, and reach of ceasefire monitoring, and reduce the risks to monitors.

In the same way that "generals always prepare to fight the last war", there is a danger of applying conventional and outdated thinking to resolving the challenges of monitoring a ceasefire in a digital age. Even the recent experience of the OSCE SMM has limited relevance, both because the conditions today are significantly different than when the SMM was deployed and because technology has made rapid advances in the past four years. Therefore, it is worthwhile to push the boundaries when thinking about the possible application of technology for ceasefire monitoring and verification.

In addition to human patrols or stationary observation posts, the advantages of deploying remote sensing technology such as cameras, uncrewed aerial vehicles (UAVs), radar and various types of sensors include:

- increasing the volume and quality of available data in the area being monitored;
- increasing the range of coverage to places that are hard to reach for human monitors, e.g. due to denial of access, topography, the presence of mines, active combat, or dangerous conditions (such as sites that contain nuclear or other hazardous materials);
- enabling 24/7 monitoring (which is important because many ceasefire violations occur at night);
- increasing the probability that violations will be detected;
- monitoring "depth areas" and limitation zones well behind the front lines, particularly for verification of the separation of forces and withdrawal of heavy weapons; and
- mitigating allegations of bias or inaccuracy that human monitors are confronted with.[6]

Overall, if done properly and as part of a functioning monitoring architecture, the use of technology for ceasefire monitoring can help to create a clearer, more accurate, and more comprehensive picture of what is going on. It also increases the situational awareness of monitors, which can improve their operational effectiveness and enhance the mission's force protection. Furthermore, technology can help decrease uncertainty around serious violations and enable a rapid response to reduce tensions.[7]

In theory, if the parties feel that they are being watched, there should be a lower likelihood of ceasefire violations. In that respect, technology can enhance violence

6 Hug, 2024, p. 12.

7 Charap et al., 2025, p. 55.

prevention or containment.[8] Indeed, this is perhaps why monitoring hardware such as cameras and drones used by the SMM was targeted by combatants: it was an attempt to blind the international community.

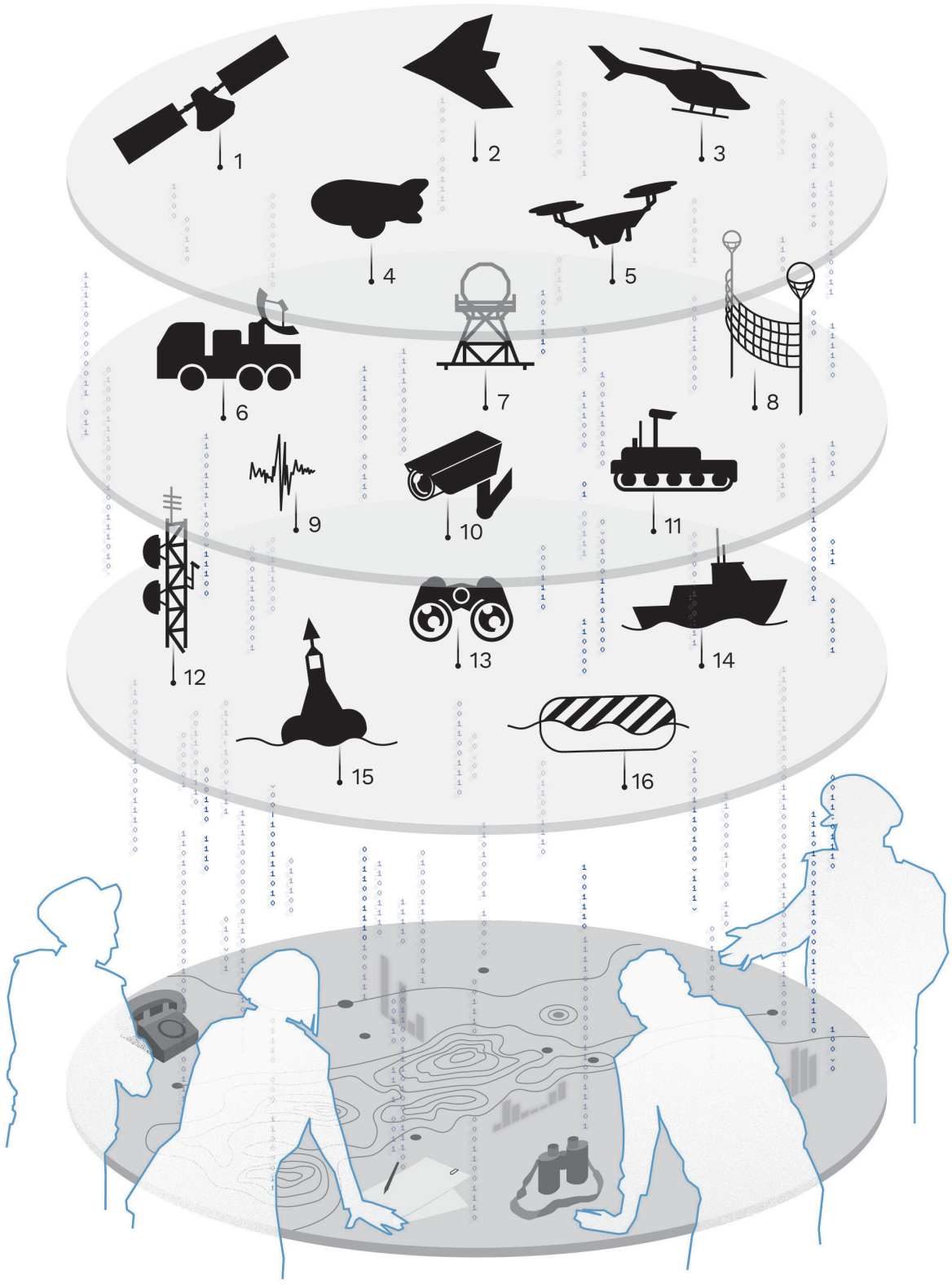
That said, using technology to strengthen compliance is only credible if there is a follow-up mechanism that holds violators accountable for ceasefire violations. Otherwise, technology just provides real-time reporting of bad behaviour, with no consequences, which undermines the credibility of the ceasefire and the monitors. For these reasons, a joint military commission will be vital.[9]

8 Hug, 2024, p. 135.

9 GCSP, 2025, pp. 12-15.

A multi-layered and integrated monitoring system

Technology for ceasefire monitoring should cover the domains of land, air, and sea, and perhaps cyberspace. It should complement human monitoring.



The technology should be part of a multi-layered and integrated monitoring system.

Air:

1. Satellites
2. Long-range uncrewed aerial vehicles (long-range UAVs)
3. Fixed-wing aircraft and helicopters
4. Tethered aerostats
5. Medium- and short-range uncrewed aerial vehicles (medium- and short-range UAVs)

Land:

6. Portable radar
7. Aerial surveillance radar systems
8. Anti-drone nets between tethered aerostats
9. Seismic, acoustic and motion sensors
10. Visual sensors (e.g. PTZ cameras)
11. Uncrewed ground vehicles

Sea:

12. Coastal surveillance radar
13. Human monitors on site
14. Ships or uncrewed vessels
15. Offshore surveillance buoys (with cameras or sensors)
16. Floating boom barriers

Coordination centre

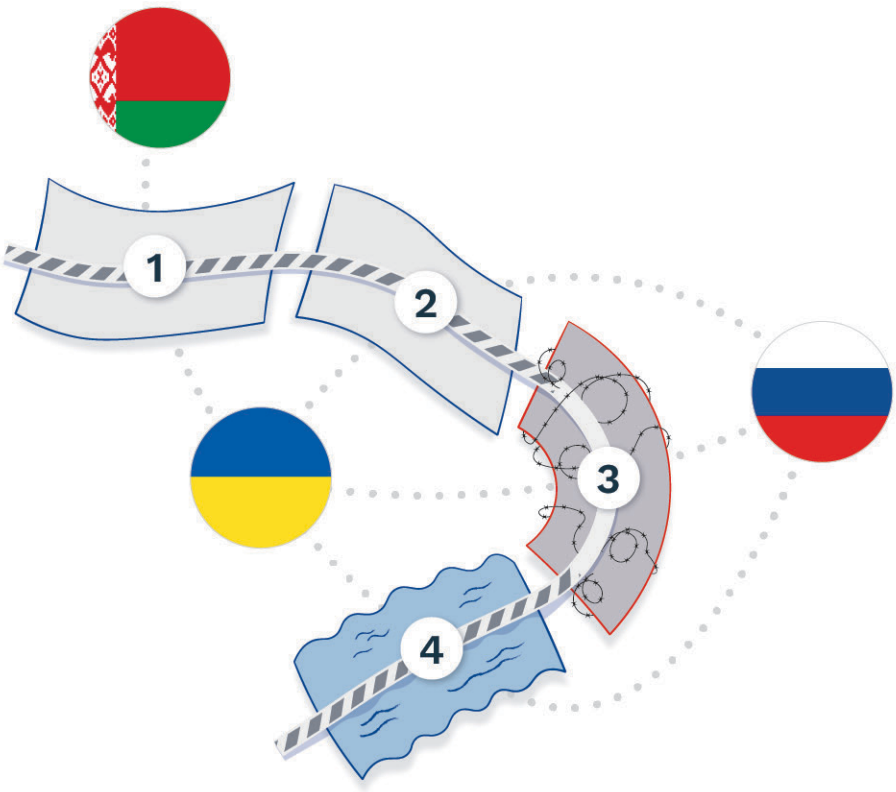
Information gathered by this technology and human monitors should be fed into a coordination centre in a way that is reliable, trusted and equally accessible by the parties. Third parties may be necessary to help with information gathering (monitoring), verification and analysis of the data.

A description of many of these types of equipment, as well as their advantages and disadvantages, can be found in the RAND Corporation report on *Guidelines for Designing a Ceasefire in the Russia-Ukraine War*[10] and a publication by Sarah Grand-Clement at UNIDIR on *Exploring the Use of Technology for Remote Ceasefire Monitoring and Verification*.[11]

As has been pointed out, "while no single remote-sensing technology can be used to monitor the disparate geographies of the conflict line, a combination of remote-sensing capabilities and platforms could achieve a persistent and pervasive presence capable of responding to emergent monitoring needs". [12] Therefore, a multi-layered approach can achieve the best results. Of course, this should be combined with monitoring by humans.

Different types of technology serve different purposes, and some are more suitable for certain types of terrain or function than others. The RAND report points out different needs and options in different sectors, including Ukraine's northern borders with Belarus and Russia, the conflict line and surrounding areas, and along Ukraine's coastline and the Dnipro river.[13]

Different sectors for ceasefire monitoring



10 Charap et al., 2025, pp. 78-100.

11 S. Grand-Clement (2022) *Exploring the Use of Technology for Remote Ceasefire Monitoring and Verification*, UNIDIR, https://unidir.org/publication/exploring-the-use-of-technology-for-remote-ceasefire-monitoring-and-verification/.

12 Charap et al., 2025, p. xi.

13 Ibid., pp. 65-77.

In some of these zones, e.g. along Ukraine's internationally recognised borders with Belarus and the Russian Federation, the type of modalities and equipment may be significantly different than along the buffer or demilitarized zone or in maritime areas. Furthermore, some sectors (such as sectors 3 and 4) may require third-party monitoring, whereas others (such as sectors 1 and 2) may not.

In areas with civilian populations, visual sensors could be mounted in strategically important positions. Cameras, either mounted on fixed masts, buildings, or observation towers, or positioned on tethered aerostats, could be placed at important crossings or key infrastructure, e.g. in the security zone. Pan-tilt-zoom (PTZ) systems with large optical zoom, 360-degree coverage and thermal sensors would be particularly effective.

Areas that are harder to access, e.g. because of the presence of mines or explosive remnants of war, or which are in "deep areas" well away from the line of contact, could be monitored by UAVs. These would include short-range tactical UAVs, such as small quadcopters with a range of 5 km. In the context of ceasefire monitoring, they are suitable for mobile patrol units and verifiers who could deploy them from their vehicles to enhance real-time situational awareness. Their small size and manoeuvrability make them ideal for deployment in urban and forested areas. Medium-range UAVs have a longer range and can carry a heavier payload than their short-range counterparts, e.g. some can fly 150-200 km for up to six hours with a payload of 30-50 kg. They could be particularly effective for verification. Long-range UAVs can fly for 20 or more hours with a range of at least 200 km, and can carry a payload of between 150 and 300 kg.

Since technology is advancing very quickly, a ceasefire monitoring operation in Ukraine should seek to innovate. For example, uncrewed ground vehicles (UGVs) equipped with cameras could be used to monitor dangerous areas or detect mines. If fast enough, they could also be a lead vehicle in a patrol. With regard to verification, weapons that are withdrawn or decommissioned could be de facto locked down through a perimeter intrusion detection system that would detect any movement into or out of a designated area. The perimeters of a demilitarised zone could be lined with a variety of sensors. Whereas in the past, e.g. in the Middle East, the UN has often simply painted barrels to demarcate a withdrawal line – such as the Blue Line between Israel and Lebanon – it could be worth experimenting with "smart markings", such as a clearly marked object (including a light and even a camera) that would demarcate a withdrawal line and enable a degree of monitoring at the same time. A similar method could be piloted with buoys in maritime regions.

In the past few years, significant advances have been made that could enable geophysical techniques, such as seismo-acoustic analysis, to contribute to ceasefire monitoring. As has been pointed out, analysing small vibrations in the earth or air, drawing on technology already used to monitor implementation of the Comprehensive Nuclear-Test-Ban Treaty, a seismo-acoustic monitoring system could help detect conflict-related explosions and provide basic coverage of the entire conflict zone, including areas not extensively monitored by other technologies.[14] It is worth noting that seismic equipment on land can detect

14 B.D.E. Dando et al. (2025) *Widening the Ceasefire Toolkit: The Promise of Geophysical Monitoring in Ukraine and Beyond*, London,

explosions at sea. Distributed acoustic sensing could be used for cantonment areas (weapons) and along the line of contact.[15] Integrating seismic and infrasound data with data from audible-frequency (short-range) acoustic sensors could help with attribution.

In short, a wide range of technological options are available for ceasefire monitoring and verification.

European Leadership Network, p. 4.

15 Ibid., p. 10.

Technology in context

There is a great deal of hype about the potential role of technology in ceasefire monitoring. While it can be beneficial for all of the reasons listed above, its usefulness should be seen in context.

Firstly, technology cannot realistically monitor every kilometre of a vast area, although it can cover a much wider area more safely than human monitors. Secondly, as experience has shown, "more information does not automatically lead to greater compliance without an agreed attribution and follow-up mechanism".[16] Therefore, technology should be used to feed information into a system that enables accountability, such as a joint coordination mechanism, ideally with third-party engagement. Technology should also be integrated into monitoring and verification operations, and should not be regarded as a standalone capacity.[17] Related to this point is the fact that the use of technology should be purpose driven, and the right tools should be selected for the appropriate functions and suitable locations.

Furthermore, it is important not to create a hierarchy between information gathered by technology compared to that gathered by civilian monitors. By putting too much faith in technology, there is a risk that the parties may shirk responsibility for violations documented without the use of remote-sensing technology.[18]

Installing technology will pose some logistical challenges. For example, any laying of fibre-optic cable would require a trench to be dug, including close to the front line. A geophysical ceasefire monitoring system would require the installation of arrays and sensors, some of which would have to be buried in bunkers.[19] Cameras, UAVs, and aerostats can be targeted and put out of action (see below). Furthermore, the effectiveness of some types of technology, such as cameras mounted on UAVs, can be hindered by bad weather or topography. Maritime ceasefire monitoring is relatively uncharted waters.

It must be stressed that technology, however useful it may be, should be considered as a complement to, rather than a replacement for, human monitors. It is an enabler, not a panacea. Human beings will be needed to:

- provide qualitative assessments of local conditions;
- engage with affected communities for reassurance, assessing local needs and understanding local contexts;
- demonstrate a physical presence on behalf of the international community;
- build local trust and buy-in for the ceasefire-monitoring process;
- operate and maintain the technology used for monitoring, and analyse and report on the data that it produces; and

16 Hug, 2024, p. 61.

17 Ibid., p. 13.

18 A. Verjee (2025) "How Surveillance Motivates New Violence: Ceasefire Monitoring, Remote Sensing Technology, and Noncompliance", *Surveillance & Society*, 23(3), pp. 287-302.

19 Dando et al., 2025, p. 14.

- foster military-to-military dialogue on ceasefire monitoring and verification, including the use of technology and negotiating access.

Since technology, particularly drones, has terrorised local populations in Ukraine for almost a decade, human monitors can play a key role in assuaging fears and distrust about the use of similar technology for monitoring. A personal touch is also vital, both to provide reassurance to local populations that have lived through a decade of violent conflict and in interaction with the armed parties. Civilian monitors can also pick up valuable situational insights from talking to locals and the respective militaries.

Therefore, human monitors and experts are vital for simply being present, for engaging with the conflict-affected population, for granular monitoring, and for deploying and maintaining the technology used for monitoring, as well as for managing and analysing the information gathered by this technology. Smart monitoring requires smart monitors – personnel with specialised skills to use the available technology. It may be necessary, as was the case in the SMM with pilots of long-range UAVs, that the companies that produce the technology may also have to provide experts to operate and service it. This needs to be taken into account in relation to a related human resources policy, accountability, duty of care and chains of command.

It is vital to underscore that what is technically feasible is not always politically possible. One or both of the opposing sides may resist the use of certain types of technology, especially if such equipment is considered intrusive. The consent of the parties to deploy certain types of technology, such as long-range UAVs or satellite imagery, is vital. Otherwise, what is meant as transparency- and confidence-building measures may turn into trust-breaking ones. For example, as the OSCE learned during its monitoring in Ukraine between 2014 and 2021, there is a fine line between the perception of monitoring versus intelligence gathering.[20] Suspicion is sometimes raised as to the question "who is watching?" In short, the consent of the parties to deploy technology for monitoring and verification purposes is vital.

But the parties will have to justify their positions, and trade-offs may be necessary. For example, if one side opposes the use of high-end technology, then they should allow more human monitors to be deployed. Conversely, if one side opposes a large number of monitors, then they should accept more technical control methods.

That said, the deployment of technology can be a key confidence-building measure. In general, "by accepting compliance mechanisms that make it harder to cheat, conflict parties can signal their seriousness about compliance".[21] As a practical example, parties may have a self-interest in installing sensors on their side of the contact line, since such technology is most likely to detect violations by the opposing party.[22] This literally builds in an element of reciprocity. The sides would

20 Hug, 2024, p. 108.

21 V. Sticher and A. Verjee (2023), "Do Eyes in the Sky Ensure Peace on the Ground? The Uncertain Contributions of Remote Sensing to Ceasefire Compliance", *International Studies Review*, 25(3), p. 4.

22 Dando et al., 2025, p. 14.

also have to work together to analyse information and follow up on incidents. They could also agree on overflights to carry out verification.

Following on from this point is the need for specific modalities and rules of engagement to be spelled out and agreed upon concerning the use of technology for monitoring and, if possible, verification. Indeed, the use of technology for monitoring should be part of the ceasefire agreement, or agreed as a supplement to it. For example, roles and responsibilities, as well as types of equipment; the use of drones; and how information is collected, managed, and shared must be clearly spelled out. While ambiguity can help efforts to reach a political agreement, when negotiating a ceasefire, technical precision is crucial. Conversely, in the field of ceasefires, ambiguity kills.

The question also needs to be asked as to whose assets will be used for monitoring. Can it be left to the opposing sides to monitor the ceasefire? After all, both Ukraine and Russia have an abundance of capacity and experience in the use of remote-sensing technologies for intelligence gathering, surveillance, and reconnaissance.[23] If monitoring were to be carried out solely by the opposing sides, the management, analysis, sharing and reporting of information will be crucial. That said, in the current situation and due to the fundamental lack of trust between the respective militaries, it is hard to imagine that such information exchanges and incident follow-up could be done in a purely bilateral format. There could also be disagreements about monitoring and verification on the opponent's side of the border or contact line. Any ceasefire violation could also lead to the trading of accusations and an escalation of tensions, or even a resumption of violence. To reduce bilateral tensions caused by monitoring, at the very least some sort of low-threshold third-party support is advisable. More realistic would be the deployment of an international ceasefire monitoring mission with its own assets. The nature of those technological monitoring assets and how they can be used will play a vital role in determining the composition of the mission. For example, in addition to civilian monitors, it may be necessary to deploy military units and/or private contractors who have the necessary skills and equipment.

Therefore, while Russia and Ukraine may possess an abundance of assets that could be used for monitoring a ceasefire, third parties will be vital to build trust and provide unbiased reporting. And they will need their own assets for third-party monitoring – "to provide the referee with better binoculars", as the RAND report puts it. In short, if technology is to be part of ceasefire monitoring in Ukraine, it will require third parties to collect, analyse and verify the information – in close cooperation with the parties to the conflict.

23 Charap et al., 2025, p. 51.

Tech as a target

The experience of the OSCE SMM shows that the technology used for monitoring can be targeted by the parties. This included shooting at cameras or drones, or interfering with UAVs.[24] Aerostats would also be a tempting target. Such attacks are both disruptive and expensive. There can also be digital threats such as jamming, spoofing and anonymous drone incursions.[25] As has been pointed out, such violations are often considered by conflict parties to incur a lower cost than resisting classical forms of (human-focused) monitoring. Furthermore, targeting remote-sensing technology is a way of "testing" monitors' surveillance capacities and their reactions and resolve.[26] Therefore, the use of technology for monitoring may in some cases trigger rather than deter violence. It should be added that the presence of human monitors can also sometimes increase ceasefire violations – what has been referred to as "third-party signaling violations".[27]

In the four years since the OSCE SMM withdrew from Ukraine, both Russia and Ukraine have significantly increased their capacity to evade, disrupt or disable remote-sensing equipment and to carry out drone attacks. Therefore, any monitoring and verification equipment belonging to international monitors should be clearly marked (e.g. with a specific colour and/or symbol) and, if necessary, send out visible or audible signals (such as flashing lights or a distinct noise or using a transponder) to distinguish their impartial function and warn any potential violators.[28] Furthermore, attacks on monitoring equipment should be considered a ceasefire violation, and be treated as such.

Any international monitoring mission should prioritise UAV procurement, and have contracts that enable rapid adaptation and frequent repairs, modifications, and upgrades. More generally, any monitoring mission will require a tech-savvy and proportionate support team.

As technology becomes more sophisticated, there is a real risk that one of the parties could hack into or tamper with the data collected, either to mask its own violations or to seek to discredit the other side. This can be overcome with the use of "verified imagery" (a type of digital watermark) to avoid fakes.[29] Chain-of-custody safeguards will also be necessary to guard and maintain the integrity of the information being gathered and shared. Embedding AI and blockchain into the monitoring architecture can also enhance confidence in the data. Indeed, data security is vital to ensure that the parties trust the monitoring system.

24 Hug, 2024, pp. 176-180.

25 B. Cook (2025) "Drones, AI, Blockchain and the New Architecture of Monitoring", Sarcastosaurus, 30 November, https://xxtom-cooperxx.substack.com/p/drones-ai-blockchain-and-the-new.

26 Verjee, 2025.

27 Sticher and Verjee, 2023, p. 8.

28 Charap et al., 2025, p. 94.

29 Hug, 2024, p. 151.

A UAV-free zone

The use of UAVs, such as first-person view (FPV) drones, fixed-wing one-way attack UAVs and surveillance UAVs, has been a defining feature of the war in Ukraine. If a buffer zone is to be established, a major challenge will be to keep it drone free, or at least to restrict drones from flying below an agreed altitude (such as 3,000 metres). Indeed, any country contributing monitors would want to be reassured that their nationals would not be attacked by drones. But the high availability of a wide range of cheap drones lowers the threshold for the parties and rogue actors to harass each other with one-off attacks or orchestrate false-flag incidents. Therefore, clear restrictions on the use of drones must be part of any ceasefire agreement.

Ideally, an agreement would stipulate that both sides would not fly any drones into a demilitarised zone. It would also oblige the parties to withdraw their electronic warfare and air-defence systems to a distance where they could no longer threaten UAVs in the security zone. At the same time, any agreement involving third-party monitoring should enable the use of UAVs by the international monitors and verifiers. Any aerial assets used by third-party monitors would have to be clearly identifiable as non-targets. Consequently, the use of physical markings, distinctive colours, and radio transponders would have to be negotiated and implemented.

This would have to include agreement on radio frequency (RF) monitoring and management that would create a predictable airwave environment where monitors could fly without obstructions and intruders would be detected early. A small number of pre-approved "green lane" channels could be reserved for third-party monitors. Along the perimeter of the demilitarised zone (DMZ) or security zone, passive radio detection nodes could be set up to continuously listen across common RF/video transfer bands, flagging any unauthorised emissions. If authorised, monitors could apply geofenced channel-specific denial (jamming) against the intruder's link while protecting the green lanes. All RF events can then be time synchronised and logged alongside video/radar tracks to support transparent incident reporting and de-escalation.

Artificial intelligence could help. For example, as has been suggested,[30] every authorised drone could send a unique, rapidly rotating digital signature (or "squawk"). The signature would be registered on a shared ledger with the parties (and any agreed third parties). Each digital signature could be secured by blockchain immutability, making it hard to spoof. In this way, any drone flight can be authenticated instantly and transparently, while any rogue drone lacking the correct signature would immediately trigger an alarm.[31]

Since it is unlikely that the monitors would have an enforcement mandate (*inter alia* to shoot down drones), it is more realistic that they would have limited measures for force protection such as RF monitoring and management, as well as radar detection. Monitors would need equipment to locate intruding drones,

30 Cook, 2025.

31 Ibid.

classify them and identify their trajectory. For this, advanced PTZ cameras along the edge of the buffer zone would be crucial. Drone detectors and purpose-built radar systems for countering uncrewed aerial systems would also be vital. The next level would be the capacity to use signal jamming to break the control and video links of unauthorised drones inside the DMZ.

Since RF monitoring and signal jamming are not 100% reliable; fibre-optic cable-controlled drones are immune to signal jamming; and FPV drones possess a lethal, yet plausibly deniable danger to monitors' lives, the monitoring mission may have to train and equip monitors with anti-drone guns and drone interceptors. Physical barriers such as drone cages on vehicles and nets stretched around observation posts and checkpoints may also be necessary. The creative use of tethered aerostats, e.g. linked together by bird-safe netting and lined up along key sectors of the buffer zone, could also be an effective last-resort barrier to prevent low-altitude drone attacks.

Maritime monitoring

The same principles used for monitoring on land could be applied at sea, although some of the technology and other monitoring assets would be different. That said, the information collected should still be part of an integrated monitoring system.

Again, as with other aspects of monitoring, the starting point should be to establish what needs to be monitored. Would there be monitoring of maritime zones extending from a coastline, such as the 12 nautical-mile limit? Would there be monitoring of ports or inland waterways? Would there be agreement on exclusion zones and passage corridors?

The ground-breaking but short-lived Black Sea Grain Initiative showed that the parties are able to agree on measures of mutual interest, such as the export of Ukrainian grain, Russian food, and fertilisers, creating a humanitarian corridor for the safe passage of ships and preventing attacks on merchant and civilian vessels. It is worth noting that the implementation of the deal was supported by a Joint Coordination Centre, with representatives from all parties, that was responsible, *inter alia*, for developing operational plans, managing vessel registration, and monitoring ships.

Depending on the monitoring mandate, naval patrols may be necessary. This may be particularly important if and when Türkiye re-opens the Turkish Straits to military vessels, since Russia could quickly strengthen its military presence in the Black Sea while others would be at a disadvantage because of provisions of the Montreux Convention.

Again, depending on the tasks, coastal surveillance radar (CSR) could be deployed to monitor and track movements along de-escalation zones in the Black Sea. CSR systems, which are commonly used by ports, ferry terminals, lighthouses, and fisheries, are readily available for civilian and commercial purposes. They commonly have a range of 180-200 km.

Subject to mutual consent, cameras and CSR systems could be installed on islands in the Black Sea. It is worth noting that in 2022, remote-controlled cameras replaced members of the Multinational Force of Observers on the tiny island of Tiran in the Gulf of Aqaba.[32] Is this model transferable to the Black Sea or the Dnipro river?

Another common tool that could be deployed for maritime ceasefire monitoring is offshore surveillance buoys. They could be used for the demarcation of passage corridors and mines, and mounted on floating boom barriers that could be deployed to create exclusion zones. They could also be outfitted with a variety of sensors – from cameras, to radar, to acoustic systems. Many models come equipped with solar panels, ensuring long endurance and autonomous operation.

In theory, uncrewed surface vessels and uncrewed underwater vehicles or drones could be used for monitoring, e.g. for underwater monitoring, and mine detection

32 Al Jazeera (2022) "Cameras to Replace Peacekeepers at Red Sea Tiran, Sanafir Islands", 21 July, https://www.aljazeera.com/news/2022/7/21/cameras-to-replace-peacekeepers-at-strategic-red-sea-islands.

and clearance. But they are relatively expensive, and their use as weapons of attack (especially by Ukraine) during the war would make both sides highly suspicious of any such crafts in their vicinity.

What to do with the information?

Tech-enabled ceasefire monitoring can generate a vast amount of data. Therefore, gathering information will be only half the challenge: the other half is the management and security of that information. This will require an integrated information management system. After all, as has been pointed out, "the use of technology is only as good as the systems put in place to process the vast amounts of information".[33]

An integrated information management system would need to be designed in a way that would enable the parties to input information and access it. There would have to be tight security protocols that are respected by the parties to ensure that they trust the system.

It would be necessary to have a team to analyse the information and report on it. While both sides would have to be engaged, impartial third parties could be helpful to assist with analysis. In this respect, it could be helpful to establish a fusion or information management centre for data integration and analysis. Artificial intelligence could be used to help synthesise information. This centre could be in a third country. Indeed, such a centre could de facto be a key element of third-party support.

There is a high risk that after such a hotly contested war and a potentially messy peace, a purely bilateral reporting mechanism would deteriorate into a "he said, she said" series of accusations. This is another reason why third-party support is important. Having a joint coordination mechanism mandated by and overseen by a "mother organisation" such as the UN, OSCE or a *sui generis* arrangement would enable an escalation of political pressure in the case of serious ceasefire violations.

It will be vital to agree on what constitutes a ceasefire violation, e.g. reporting on every single burst of small arms fire would be untenable.

Crucially, procedures would also have to be put in place to investigate serious ceasefire violations. This could include a technical response, such as sending up a drone, as well as deploying monitors and/or representatives of the parties, such as a "three-in-a-jeep" model.

A tricky issue would be attribution. If ceasefire monitors or monitoring equipment record a ceasefire violation, the parties would have to investigate the incident. In the process of trying to ascertain what happened, there would be strong pressure to determine who is at fault, especially if violations have significant consequences.

The parties would have to agree on modalities for reporting, such as frequency and types of reports, who would receive this information, and whether it would be made public. A lesson learned from making reports public is that listing ceasefire violations without specifying attribution can result in the parties

33 A. Hug and S. Mason (2022) "Ceasefire Monitoring and Verification Technology", *CSS Policy Perspectives*, 10(2), p. 3.

selectively highlighting information from monitoring reports to blame the other side for violations or to call into question the objectivity of third-party monitors.

Modalities would also have to be agreed on how to store information. This is not only important for keeping records, but also for monitoring trends or changes over time.[34]

34 Ibid.

A cyber ceasefire?

While ceasefire monitoring is traditionally concentrated on what goes on in the physical world – on land, in the air and at sea – warfare between Ukraine and Russia has also been carried out in a fourth domain, namely in cyberspace. For example, Russia has been accused of carrying out a cyber attack on Ukraine's Viasat satellite communication network in 2022 and the Kyivstar Telecom in 2023, while Russia has accused Ukraine of carrying out cyber attacks on its federal tax service and the M9 Telecom.

If this has been a cyber war, does there also have to be a ceasefire in cyberspace, and what would this look like?[35] There are few precedents to draw on in terms of inter-state ceasefire agreements. There are also inherent risks, such as overloading an already complex ceasefire agreement with even more variables, the challenge of attributing responsibility for cyber attacks, and the danger that a cyber attack by rogue elements could unravel a fragile ceasefire. It is also very easy to break a cyber ceasefire and very difficult to monitor one. In short, it is probably best to keep any steps designed to reduce offensive cyber operations separate from a ceasefire agreement.

That said, as has been pointed out in one of the few studies on cyber ceasefires, excluding the cyber domain risks creating confusion about what is and is not prohibited under the ceasefire, and would create ambiguity that could be exploited by the parties or spoilers.[36] Therefore, "we need to invest in ceasefires that don't just address the physical and ignore the digital".[37]

With this in mind, at a minimum it is worthwhile to raise the issue of restraint in relation to offensive cyber attacks; acknowledge the issue in the context of negotiating a ceasefire; explore the possibility of including definitions in the ceasefire agreement on what constitutes a cyber attack; and, if possible, introduce basic principles of constraint on cyber operations and a commitment by the parties to cease offensive cyber activities.[38] A more ambitious agenda would explore how to monitor a cyber ceasefire.

Because the issue is rather technical, it may be advantageous to discuss modalities among relevant experts from both sides, apart from negotiations on other possible elements of a ceasefire. It may also be necessary to involve third parties. There could also be merit in drafting a standalone cyber de-escalation agreement,[39] although if that were the case there should be a link to the broader ceasefire agreement and, potentially, any framework agreement or political settlement.

35 S. Kane and G. Clayton (2021) *Cyber Ceasefires: Incorporating restraints on Offensive Cyber Operations in Agreements to Stop Armed Conflict*, Zurich, Center for Security Studies (CSS), ETH Zurich.

36 Ibid.

37 B. Solomon and B. Popken (2025) "For True Peace, Ceasefires Must Address Digital Warfare, Too", Tech Policy Press, 9 July, https://www.techpolicy.press/for-true-peace-ceasefires-must-address-digital-warfare-too/.

38 Kane and Clayton, 2021, pp. 40-49.

39 Ibid., p. 25.

Where to start?

Ceasefire monitoring in Ukraine will require a multi-domain and multi-layered approach enabled by technology. However, all of this cannot be done at once, nor is it realistic that the several thousand kilometres of borders, contact lines and depth areas can be comprehensively monitored. Therefore, it is important to manage expectations, have a sense of the potential bigger picture, but start in a step-by-step way.

For example, one of the first steps would be to encourage the parties to discuss bilaterally (with third-party support if requested) what needs to be monitored and for what purpose, and only then initiate a discussion on how technology can help to reach those objectives. Building on such introductory talks, the parties, ideally with third-party support, could initiate bilateral discussions about modalities for the use of technology for ceasefire monitoring and verification, drawing on good practices. They could also explore together how technology can be used for ceasefire monitoring in ways for which there is less international experience to draw on, e.g. maritime ceasefire monitoring and how to create a UAV-free zone.

Technology could be piloted to monitor local ceasefires. As has been pointed out, "early on in a peace process, simple technology systems may help in monitoring short-term humanitarian ceasefires or temporary pauses in fighting".[40] Technology could also be used to monitor local ceasefires and a temporary ceasefire around civilian nuclear power stations.

Operationally, to enable ceasefire monitoring, one of the first steps would be to use technology to carry out demining and to get the parties to withdraw their electronic warfare equipment far enough from the buffer zone so that it could not interfere with UAVs operated by international monitors. Such a move would be a leap of faith for both sides, but would be a strong signal of their intent to create an enabling environment for a ceasefire.[41]

Because technology is developing quickly and could revolutionise ceasefire monitoring, organisations such as the UN and OSCE that could be involved in ceasefire monitoring in Ukraine should begin contingency planning to look at what possible assets would be needed and where and how they could be procured, and define the profiles of the necessary operators.

To conclude, when a ceasefire is agreed between Ukraine and Russia, it could trigger one of the biggest and most important ceasefire-monitoring operations of all time. While the area to be covered will be large and the political stakes very high, the number of human monitors will probably be low. Therefore, technology will play a key role.

40 Hug and Mason, 2022, p. 3.

41 For more on signalling intent and a conceptual framework for ceasefire monitoring and the role of technology, see Sticher and Verjee, 2023.

Building Peace Together

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-038-9

30 YEARS GCSP Geneva Centre for Security Policy