EXPLORING THE USE OF TECHNOLOGY FOR REMOTE CEASEFIRE MONITORING AND VERIFICATION

Sarah Grand-Clément

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

ACKNOWLEDGEMENTS

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This report is the first joint report produced by the Conventional Arms and Ammunition Programme and the Security and Technology Programme of UNIDIR. This joint project, which recognizes the increased convergence between technology and conflict prevention, has been supported by generous funding for the Conventional Arms and Ammunition Programme by Germany and for the Security and Technology Programme by Germany, the Netherlands, Switzerland and Microsoft.

The author wishes to thank the experts who participated in the research through interviews or the validation workshop and provided valuable inputs during the course of the research. The author also extends her thanks to Simon Yazgi, who was the catalyst for this study and supported it throughout, as well as to Francesca Batault, who provided valuable research support. The author is also grateful to the experts who reviewed the report: Andreas Hirblinger, Georg Stein, Simon Yazgi, Paul Holtom, Giacomo Persi Paoli and Barbara Morais Figueiredo. Layout and Design by Nicolas A. Quiroga.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to a variety of existing and future armaments, as well as global diplomacy and local tensions and conflicts. Working with researchers, diplomats, government officials, NGOs and other institutions since 1980, UNIDIR acts as a bridge between the research community and Governments. UNIDIR activities are funded by contributions from Governments and donor foundations.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

Credit for cover image: UN Photo/ John Isaac

www.unidir.org

About the author

Sarah Grand-Clément is a Researcher working in both the Conventional Arms and Ammunition Programme and the Security and Technology Programme of UNIDIR. She coordinates the technology and conventional arms control workstream. Her areas of expertise include international security, new and emerging technology and its impact on international security, counter-terrorism, and futures methodologies, in particular horizon scanning, serious gaming and future scenarios. Prior to joining UNIDIR, Sarah was a Senior Analyst at RAND Europe, where she conducted defence and security policy research. She holds a master's degree in Arab World studies from Durham University and a bachelor's degree in international relations from Sussex University, both United Kingdom.

About the research team

Simon Yazgi is a Senior Advisor at the United Nations Integrated Transition Assistance Mission in Sudan (UNITAMS). He is also a senior non-resident fellow at UNIDIR where in 2019, as a member of the Conventional Arms Programme, he helped to launch UNIDIR's workstream on Integrating Conventional Arms Control into Conflict Prevention and Management. Prior to this he was the senior advisor on security arrangements in the United Nations Stand-by Team of Senior Mediation Advisors and the Chief of Disarmament, Demobilization and Reintegration (DDR) in the United Nations Department of Peace Operations. Simon has over 20 years of experience in peacemaking and peacekeeping with the United Nations in the field and at headquarters. His areas of expertise include conflict prevention and management, ceasefires, peace mediation, DDR, security sector reform, conflict analysis, Small Arms and Light Weapons control and political risk analysis.

Francesca Batault is a former Graduate Professional with UNIDIR's Conventional Arms Prior to joining UNIDIR, Batault worked for the International Crisis Group, the International Peace Institute as well as the International Committee of the Red Cross. She holds a master's degree in international relations from the London School of Economics and Political Science (LSE) and a bachelor's degree with honours in politics, philosophy and economics from Northeastern University, Boston, United States.

TABLE OF CONTENTS

Executive summary 1

1. Introduction 6

1.1 Ceasefires and conflict prevention 6
1.2 Embedding technology into ceasefire monitoring and verification 8
1.3 Purpose and scope of this study 8
1.4 Methodology 9
1.5 Report structure 9

2. Uses of technology in remote ceasefire monitoring and verification 12

2.1 Ceasefire activities 12
2.2 Technologies for remote ceasefire monitoring and verification 13
2.3 Mapping technologies to the ceasefire activities 19

3. Guiding considerations for the use of technology in remote ceasefire monitoring and verification 24

3.1 Suitability 24
3.1.1 Initial considerations 24
3.1.2 Contextual knowledge 26
3.1.3 Implications of technology use 27
3.1.4 Limitations of technology 28
3.2 Deployability 29
3.2.1 Practical considerations 29
3.2.2 Data management 29
3.2.3 Cost considerations 30
3.2.4 Level of technological knowledge 31
3.3 Governance 31
3.3.1 Trust in technology 31
3.3.2 Security of the technology and the data acquired 32
3.3.3 Ethics and privacy 33
3.3.4 Data sharing 34

4. Conclusion 36

Appendix A. Detailed overview of the technologies 40

Appendix B. Research participants 56

References 60

List of abbreviations and acronyms

AI	Artificial intelligence
DPPA	Department of Political and Peacebuilding Affairs
GIS	Geographic information systems
ICRC	International Committee of the Red Cross
IDP	Internally displaced person
MINUSCA	United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic
MINUSMA	United Nations Multidimensional Integrated Stabilization Mission in Mali
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open-source intelligence
RFID	Radio-frequency identification
SAGE	Situation Awareness Geospatial Enterprise
SMM	Special Monitoring Mission
UAV	Uncrewed aerial vehicles
UNFICYP	United Nations Peacekeeping Force in Cyprus
UNOSAT	United Nations Satellite Centre

Executive summary

Ceasefires play an important role in the prevention of further conflict and armed violence. They are a crucial component of the broader conflict-prevention toolkit and are a first step towards a peace agreement. Ceasefires with a monitoring and verification arrangement aim to build trust and collaboration between the conflict parties and avoid prohibited behaviours from taking place or recurring. They are more robust and longer lasting than similar arrangements that are not monitored.

While ceasefire monitoring and verification is usually conducted by in-person monitors, this may not always be possible due to non-permissive environments. In such instances, technology can help overcome these challenges, as well as extend the range of monitoring and the pace of data synthesis.

This report identifies 18 technologies that can be categorised as aiding with either data acquisition, data analysis or communications for remote ceasefire monitoring or verification. The term "technology" encompasses tools (both hardware and software) as well as approaches (i.e., ways in which technology can be used), to showcase a range of options drawn from different domains, including but not limited to ceasefire monitoring and verification, peacekeeping or humanitarian missions, environmental monitoring, and use by state security forces. The report maps these technologies against a set of ceasefire activities, which illustrate areas commonly subject to monitoring or verification (Figure A).

Figure A. Technologies mapped against ceasefire activities

		Weapons and ammunition	Troops and combatants	Non-lethal hostile activity	Protection of civilians	Infrastructure	Humanitarian assistance	Peacekeeping duties	Prisoners and hostages	Propaganda, hate speech and other hostile media
Data acquisition	Accoustic sensors	✓✓	-	✓	-	-	-	-	-	-
	Cameras	✓✓	✓✓	✓✓	✓	✓✓	✓	✓	✓	-
	Infrasound sensors	✓✓	-	-	-	-	-	-	-	-
	Motion sensors	✓	✓	✓✓	-	-	-	-	-	-
	Radars	✓✓	✓✓	✓✓	✓	✓✓	✓✓	✓✓	✓	-
	Satellites	✓✓	✓	✓	✓	✓✓✓	✓	✓	✓	-
	Seismic sensors	✓	✓	✓	-	-	-	-	-	-
	Aerial platforms	✓✓✓	✓✓	✓✓	✓	✓✓	✓✓	✓✓	✓	-
	UAVs	✓✓✓	✓✓	✓✓	✓	✓✓	✓✓	✓✓	✓	-
	Crowdsourcing	✓	✓	✓	✓	✓	✓	✓	✓	✓✓✓
	Data scraping	✓	✓	✓	✓	✓	✓	✓	✓	✓✓✓
	Advanced binoculars	✓	✓	✓	✓	✓	✓	✓	✓	-
	Biometrics	-	✓	-	-	-	-	-	-	-
	Cyber monitoring	✓	-	✓✓	-	✓✓	-	-	-	-
	RFID	✓	-	-	-	-	-	-	-	-
Analysis	Artificial intelligence	CROSS-CUTTING TECHNOLOGIES								
	Data fusion									
Communications										

Key: ✓✓✓ = technology very well adapted for this activity; ✓✓ = technology moderately adapted, may not be suitable for all specific areas falling under this activity; ✓ = technology has limited and/or specific areas of applicability within this activity; - = technology not suited for this activity.

Additionally, the report also identifies 12 guiding considerations (Figure B) regarding the use of technology for remote ceasefire monitoring and verification, which should be taken into account alongside the limitations and challenges of individual technologies, as well as the specific mandate of any ceasefire monitoring and verification mechanisms.

Figure B. Overview of the guiding considerations

SUITABILITY	DEPLOYABILITY	GOVERNANCE
• Initial considerations • Contextual knowledge • Implications of technology use • Limitations of technology	• Practical considerations • Data management • Cost considerations • Level of technological knowledge	• Trust in technology • Security of technology and data • Ethics and privacy • Data sharing

Based on this research, the report outlines five conclusions:

1. Combining the strengths of both technology and humans can help balance out their respective limitations. While the human element cannot be removed completely from ceasefire monitoring and verification, technology can be used to aid where needed and appropriate and if acceptable to the conflict parties.
2. Technology is flexible as to the intended function, meaning that it can be used to monitor or verify that incidents have not occurred, but can equally be used to enable dialogue or map progress made by conflict parties.
3. Technologies used to-date within ceasefires currently focus mainly on monitoring through the acquisition of data, and there has been limited use of analytical technologies. Overall, verification appears to be less suited to being achieved through the use of technology.
4. Layering of data acquisition technologies can leverage their respective benefits while offsetting their respective limitations. Layering can also help improve confidence in the data collected and means there is redundancy across the data-collection system.
5. Trust in technology plays a very important role in terms of whether one or several technologies are accepted and used in a ceasefire context.

The report also suggests several examples of good practice to consider for the future and which could be undertaken by the United Nations and other relevant entities working within the ceasefire domain:

- Promote the use of, and continuously refine and update, the guiding considerations on the use of technology in remote ceasefire monitoring and verification.
- Improve the sharing of knowledge between relevant stakeholders regarding lessons learned and the sharing of data that can enable the use of certain technologies.

- Encourage multi-stakeholder approaches to bridge the knowledge gap between the technology, ceasefire, and local experts.
- Ensure a minimum level of technological knowledge and increased familiarity of stakeholders with technologies more generally, such as on what these can offer in terms of supporting ceasefire monitoring and verification mechanisms.
- Monitor the evolution of conflicts and related ceasefire agreements to identify new areas where monitoring and verification may be required (e.g., cyberspace) in order to understand and prepare for the future of ceasefire monitoring and verification.

Cyprus, 1990 - A Gazelle helicopter flies over UNFICYP Danish contingent territory.
Credit: © UN Photo/ John Isaac

1. Introduction

1.1 CEASEFIRES AND CONFLICT PREVENTION

Ceasefires play an important role in the prevention of further conflict and armed violence. As noted by Bara et al., "ceasefires are a crucial part of the peacemaking process – a form of confidence building, means of signalling peaceful intentions, and the mechanism that sets out the terms through which armed forces transition from war to peace".[1] While there is no universally accepted definition of a ceasefire, the term broadly refers to "any arrangement in which a conflict party commits to a temporary or permanent suspension of violence".[2] Ceasefires are therefore a crucial component of the broader conflict-prevention toolkit. Ceasefires are not a stand-alone process; they need to be accompanied by the prospect of discussions or negotiations beyond the initial ceasefire agreement. As such, ceasefires are generally a first step towards a peace agreement, although it is also possible for peace agreements to be achieved without a prior ceasefire.

While a ceasefire always aims to stop or end violence, ceasefire agreements vary in scope depending on the type of conflict, context, and actors involved. Agreements can vary from looser to more rigorous arrangements between the conflict parties, which may or may not involve a monitoring element. The most commonly monitored types of ceasefire are the "preliminary" ceasefire, which aims to stop (not end) violence in order to enable negotiations, and the "permanent" or "definitive" ceasefire, which aims to end violence.[3] These two types of ceasefire are distinct from other instruments that can suspend, stop and end violence, such as humanitarian pauses, unilateral ceasefires (declared by one party to a conflict) or sectorial ceasefires (prohibiting attacks using certain weapons or on certain targets) as preliminary and definition ceasefires are usually better defined, for instance by being set out in writing and having clear timelines for implementation. By providing benchmarks according to which the parties' compliance with the ceasefire agreement can be measured, the agreement reached can be monitored and verified (see Box 1).

Ceasefires that integrate a monitoring commitment are thus "significantly more durable than other arrangements – enhancing accountability, commitment, and confidence in the process".[4] Despite these benefits, the large majority – an estimated 70 per cent – of ceasefires or instruments given this label do not have a monitoring and verification agreement in place.[5] Ultimately, the purpose of monitoring or verification functions is preventative, rather than punitive, aiming to build trust and collaboration between the conflict parties and avoid prohibited behaviours from taken place or recurring.

1 Bara et al. (2021, 329).
2 Buchanan et al. (2021, 6).
3 Correspondance with Georg Stein.
4 Buchanan et al. (2021, 4).
5 Data from the ETH/PRIO civil conflict ceasefire dataset via Bara et al. (2021).

BOX 1

Defining monitoring and verification

Monitoring involves being the "eyes and ears on the ground".[6] The elements to be monitored are defined within the agreement. Monitors act as observers on activities taking place following an agreement, gather relevant information, and report this information to the ceasefire institutions. Monitoring also involves trust-building between the conflict parties.[7]

Verification is a related but separate process. It seeks to investigate incidents, determine if they were violations of the ceasefire, and ensure that unwanted or prohibited behaviours do not occur again.

Generally, monitoring and verification occur together, with the monitoring mission gathering information which is then verified.

The actors performing monitoring and verification functions vary based on the specific ceasefire agreement but can include the conflict parties, national, regional, or international third parties, or civil society. National and international third parties include a range of actors, from states to organisations such as the United Nations, the European Union, the African Union, and the Organization for Security and Co-operation in Europe (OSCE). Civil society encompasses civilian, private individuals or non-governmental organisations reporting on incidents or alleged ceasefire violations. The composition of monitoring and verification teams can include one, several or all of these actor types, organised under a monitoring body (such as a Joint Monitoring Commission or similar set-up), and they can be civilian or military, armed or unarmed, with less or more robust mandates.[8] As with ceasefire agreements, mandates also vary in terms of their scope, the realities on the ground, as well as what is realistic and financially feasible. Mandates are negotiated by the relevant actors involved in the ceasefire process, and they define the terms of the monitoring and verification and the geographical scope of a given ceasefire.

Within the United Nations, ceasefire monitoring and verification is closely linked to peacekeeping and peacebuilding, with peacekeepers aiding the implementation of a ceasefire. Sometimes, peace missions can focus on ceasefire monitoring or they may have a wider peacekeeping mandate that includes other tasks such as protection of civilians or the political accompaniment of a peace process.[9] Where the ceasefire is not overseen by the United Nations, there may not be a broader peacekeeping mandate.[10]

6 Buchanan et al. (2021, 7).
7 Correspondance with Georg Stein.
8 Civilian teams, where the ceasefire monitors are not military or armed, are more commonly known as civilian monitoring. This is distinct from civil society monitoring.
9 Palik (2021).
10 Bara et al. (2021).

1.2 EMBEDDING TECHNOLOGY INTO CEASEFIRE MONITORING AND VERIFICATION

Ceasefire monitoring and verification is usually conducted by in-person monitors. However, this may not always be possible: monitors can be hampered from undertaking their duties, or the deployment of personnel may not even be possible. For example, in the Syrian Arab Republic in 2016, conditions were deemed too dangerous for physical monitoring.[11] More recently, in Ukraine, monitors of the OSCE Special Monitoring Mission (SMM) to Ukraine were notably prevented from leaving their patrol base.[12]

Technology cannot replace humans in the monitoring and verification of ceasefires, especially in data analysis, dialogue, and de-escalation efforts. However, technology can help overcome some of the obstacles that monitors face and can also extend the range of monitoring and increase the pace of data synthesis, if needed, if appropriate and if acceptable to the parties to a ceasefire. Most importantly, use of technology could also reduce risk of personal harm to personnel on the ground.

The use of technology has been explored in the peacekeeping domain more broadly. In 2014, the Expert Panel on Technology and Innovation in United Nations Peacekeeping released a report on technologies and innovation that could improve peacekeeping operations, at the request of the Under-Secretaries-General for Peacekeeping Operations and Field Support. Following this report, there has been an increased focus on new and emerging technologies and how they can support efforts by the United Nations, as noted by the Secretary-General's 2018 Strategy on New Technologies. Specific to the use of technology by peacekeepers, the Secretary-General noted that digital technology is critical for United Nations peacekeeping in his 2020 Roadmap for Digital Cooperation.[13] This was followed in 2021 by the Strategy for the Digital Transformation of UN Peacekeeping, which outlines a number of principles around the use of technology in peacekeeping.[14]

Yet, the technology used in peacekeeping more broadly may not transfer or apply to ceasefire contexts. While there may be some areas of overlap in the technologies and in the principles around their use, this report is solely aimed at highlighting the use of technology within ceasefire monitoring and verification, rather than within the broader peacekeeping field.

1.3 PURPOSE AND SCOPE OF THIS STUDY

UNIDIR has undertaken this study in order to identify and assess the technologies available to help monitor and verify ceasefires and in order to provide guidance to mediators and missions on how these could be used. The goal is to help strengthen the remote monitoring and verification of ceasefires and reduce risk of harm to

11 Nicols (2016).
12 Ermochenko & Polityuk (2021).
13 General Assembly (2020).
14 United Nations Peacekeeping (2020).

personnel on the ground. This report does not provide guidance on how or when technology should be discussed and integrated into a ceasefire agreement by the mediators, nor does it discuss the acceptability of the use of technological means in the monitoring or verification of a ceasefire, as these fall beyond the remit of the study.

This study is aimed at United Nations personnel working on peacekeeping, ceasefire mediation and ceasefire monitoring and verification, as well as individuals in other regional or local organisations working on ceasefires, to consider as part of ongoing and future ceasefire negotiations.

1.4 METHODOLOGY

This study involved four activities. First was a review of over 60 ceasefires agreements established between 2000 and 2021, in order to identify the most common types of activity that tend to be monitored and verified. Second was a thorough desk research, which focused on relevant peer-reviewed literature related to ceasefires, peacekeeping, technology use in ceasefires, and technology used for monitoring more broadly. This included a deep dive into four missions: the OSCE SMM to Ukraine, the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), the United Nations Peacekeeping Force in Cyprus (UNFICYP) and the United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic (MINUSCA). Third, interviews were conducted with 46 individuals working in international organisations, national governments, ceasefire missions, academia, and other research organisations as well as the private sector, with experience on ceasefires or technology. Finally, a workshop was held which brought together 15 experts in ceasefires, peacekeeping, and technology and which sought to assess, refine, and validate the research findings.

1.5 REPORT STRUCTURE

In addition to this introductory chapter, the report is comprised of three chapters:

- **Chapter 2** provides an overview of the technologies that can be used to help monitor or verify ceasefires.
- **Chapter 3** offers a series of guiding considerations regarding the use of technology in ceasefire monitoring and verification.
- **Chapter 4** concludes the report.

The report also contains two appendices. Appendix A provides a more detailed description of the technologies, and appendix B lists the interviewed experts.

Cyprus, 1990 - A member of the UNFICYP Danish contingent in Ferret Scouts approaches an observation post near Skouriotissa.
Credit: UN Photo/ John Isaac

2. Uses of technology in remote ceasefire monitoring and verification

This chapter provides an overview of the activities that ceasefires aim to monitor and verify and describes relevant technologies that can be used to undertake remote ceasefire monitoring and verification.

2.1 CEASEFIRE ACTIVITIES

To help illustrate the areas across which technology could be applied, a review of over 60 ceasefire agreements reached between 2000 and 2021 identified nine activity areas commonly subject to monitoring or verification (Table 1). This list is not meant to be exhaustive, as each agreement will be different given these are shaped by the circumstances of the conflict such as the conflict parties, any third parties, the location and time at which a conflict took place, the challenges emerging from the type of conflict, the terrain, and more. For example, in future, cyberspace may feature more prominently in ceasefire agreements than it does currently.[15] As such, the identified activities are presented in broad terms to avoid assumptions about the terms of an agreement; the (non-exhaustive) examples of the activity areas aim to demonstrate how the activities have been or could be reflected in an agreement.

Table 1. Activities commonly monitored and verified in ceasefire agreements

ACTIVITY AREA	EXAMPLE OF ACTIVITIES MONITORED AND VERIFIED
The terms of the agreement regarding **weapons and ammunition** are respected	• No use of lethal weapons in the air, on land or at sea (e.g., to ensure further territorial gains or otherwise) • No further kinetic or non-kinetic attacks • No more unlawful ownership, acquisition, resupply or transfer of ammunition and weapons • No unauthorised movement of military equipment • No more mine laying or use of improvised explosive devices • Conflict parties have cleaned and decontaminated, or facilitated the cleaning and decontamination, of areas with explosive devices • Weapons have been placed in cantonment areas • The disarmament process is ongoing as planned
Troops and combatants abide by the terms of the agreement	• No further deployment or redeployment of troops in defensive positions • Assembly or cantonment of troops is enabled • No troops movement outside the areas specified in the agreement • No further recruitment of members • The demobilization and reintegration process is ongoing as planned

15 Interview with Annika Hansen.

Table 1 Activities commonly monitored and verified in ceasefire agreements (continued)

ACTIVITY AREA	EXAMPLE OF ACTIVITIES MONITORED AND VERIFIED
No further non-lethal hostile activity is being undertaken by the conflict parties	• No reconnaissance activities conducted • Demilitarized or buffer zones, or any other special zones specified under the ceasefire agreement, are respected • No further support provided to other armed organised groups (e.g., allied militias, terrorist groups)
Civilians are protected	• No further form of harm to civilians (including sexual violence, unlawful arrests, violence, etc.) • The free movement of civilians, goods and commercial enterprises is upheld • The safe return of refugees and internally displaced persons (IDPs) is upheld
Infrastructure is not misused or targeted	• No targeting, destruction, or illegal occupancy of buildings, refugee or IDP camps, or other property • No use of civilian infrastructure for military purposes • No further building of military infrastructure (e.g., military bases) • No targeting of critical infrastructure either in-person or online
Humanitarian assistance is facilitated	• No obstruction to the delivery of humanitarian assistance • No harm to humanitarian personnel or their equipment • Checkpoints are removed • Specific humanitarian guidelines are engaged with and implemented
Peacekeeping duties are not hampered	• No prevention of international actors from undertaking their peacekeeping and monitoring duties • No harm to peacekeeping personnel or their equipment
The terms of the agreement are respected with regards to **prisoners and hostages**	• Prisoners of war, enemy combatants and hostages are released
Propaganda, hate speech, disinformation and other hostile media are not being spread	• No further spreading of hostile statements and information, both within the specific region or country and externally (e.g., diasporas)

2.2 TECHNOLOGIES FOR REMOTE CEASEFIRE MONITORING AND VERIFICATION

This section presents a non-exhaustive range of technologies available to aid with remote ceasefire monitoring and verification. In the context of this report, a "technology" is defined to include tools (both hardware and software) as well as approaches (i.e., ways in which technological means can be utilised). This broad approach is taken since tools and approaches are closely interlinked, with each feeding into the other.

The technologies presented here were obtained from a range of different domains, including but not limited to ceasefire monitoring and verification, peacekeeping and humanitarian missions, environmental monitoring, and state security forces (e.g., police and border forces). These technologies include mature technologies that have already been used or are regularly used in ceasefire or peacekeeping contexts; technologies that have not been used in the ceasefire or peacekeeping domains but have been used in other contexts; and technologies that have seen limited to no operational use in any context. While the latter two categories could include many options, technologies have been selected to ensure that they are applicable to the scope of ceasefire activities outlined in Section 2.1 and are accessible to the civilian domain (i.e., avoiding military-grade technology).

The technologies are divided into three categories:

- **Data acquisition:** Data acquisition technologies capture raw data, which then need further processing and refining through analysis. The data captured by these technologies are most relevant for remote monitoring but can also play a role in verification activities, such as by presenting proof of an activity. As such, these technologies can help with both monitoring and verification.
- **Analysis:** Using technology to collect data means that there is often a lot of information to process and analyse; this can quickly become an extremely time-consuming task. Analysis technologies can enhance the capabilities of human analysts, with a focus on technologies that can (pre)process data collected by the data acquisition technologies outlined above. Due to space and scope constraints, technologies in this category do not include individual commercial analytical tools, such as Google Earth, although these are also valid and useful tools.
- **Communications:** Communications is an essential enabling technology when undertaking ceasefire monitoring and verification. In the context of this study, communications is defined as aiding with operational information management, rather than with public affairs or social media communication.

Tables 2–4 present a short description of each technology, with detailed information available in appendix A. Boxes 2–4 discuss specific aspects of some of the technologies and how they can be combined.

Table 2. Data acquisition technologies

SUBCATEGORY	TECHNOLOGY	DESCRIPTION
Sensors	Acoustic sensors	Acoustic sensors detect and help locate the source of sounds, such as that of artillery.[16]
	Cameras	Cameras include stationary cameras, such as CCTV, as well as non-stationary cameras, which can be placed on aerial platforms such as helicopters or aircraft, including uncrewed aerial vehicles (UAVs),[17] to monitor specific areas or hotspots.
	Infrasound sensors	Infrasound sensors detect acoustic waves from 20 hertz and below, thus capturing sounds beyond the range detectable by acoustic sensors and could be used to detect explosions.[18]
	Motion sensors	Motion sensors, which can be integrated in cameras, detect movement and can also be set-up to provide an alert on suspicious movements.[19]
	Radars	Radars use radio waves to detect stationary and moving objects, for example to help detect the use of military equipment or weapons and can show the velocity of an object.[20]
	Satellites	Satellite imagery can demonstrate the evolution of a situation over time, whereby cameras on satellites take pictures from space to monitor the moving of military equipment or changes to infrastructure.[21]
	Seismic sensors	Seismic sensors capture vibrations or ground motions, such as those caused by the movement of large military equipment like tanks or even people.[22]

16 Interviews with Alexander Hug, Walter Dorn, Gary Brown, and anonymous experts E, G and H.

17 Interviews with Alexander Hug, Walter Dorn, Andreas Wittkowsky, Ajay Sethi, Margaux Pinaud, Kristin Lund, a UN official and anonymous experts F, G and H.

18 Interview with Sebastian Schutte.

19 Interviews with a UN official and anonymous expert E.

20 Interview with Walter Dorn.

21 Interviews with Kristin Lund, Alexander Hug, Annika Hansen, Patrick Loots, Walter Dorn, Camino Kavanagh, Piero Boccardo, Eliot Higgins, Ajay Sethi, Valerie Sticher, Aly Verjee, Joseph Guay, a UN official and anonymous experts A and C.

22 Interview with anonymous expert E; Clemente et al. (2019); Mukhopadhyay et al. (2018).

Table 2. Data acquisition technologies (continued)

SUBCATEGORY	TECHNOLOGY	DESCRIPTION
Aerial platforms	Helicopters, airplanes and aerostats	Crewed and uncrewed aerial platforms include helicopters, airplanes and aerostats;[23] cameras (including infrared or thermal cameras) and other sensors (e.g., radar and acoustic sensors) are usually integrated in aerial platforms to ensure weapons are not used, troops are not active or infrastructure remains unchanged.
	Uncrewed aerial vehicles (UAVs)	UAVs include fixed-wing and rotary-wing systems;[24] both types can be embedded with a range of sensors such as cameras, including with thermal and infrared capabilities, or radar.
Crowdsourcing	Crowdsourcing	Crowdsourcing enables data to be obtained from a large number of people on the ground through mobile phones or other platforms using sensor technologies.
	Data scraping	Data scraping refers to the acquisition of data from news media (written press, television, and radio) and social media, such as to understand the ongoing rhetoric.[25]
Other data acquisition technologies	Advanced binoculars	Advanced long-range binoculars are used by monitors to observe from a distance; they include sensors such as cameras and infrared, enabling the recording of data during day and night.[26]
	Biometrics	Biometrics is a form of identification and authentication of an individual, which relies on biological characteristics, such as fingerprints[27] or objects owned by individuals (token-based biometrics).[28]
	Cyber monitoring	Cyber monitoring refers to the monitoring of attacks and operations targeting digital infrastructure, including the leaking, poisoning or stealing data or the targeting critical infrastructure.[29]
	Radio-frequency identification (RFID)	RFID technology helps track items by way of tags, enabling a mass read-out of inventory.[30]

23 Interviews with Kristin Lund, Annika Hansen and Walter Dorn.
24 Interviews with Alexander Hug, Walter Dorn, Andreas Wittkowsky, Ajay Sethi, Valerie Sticher, a UN official and anonymous experts A, E, G and H.
25 Interviews with Annika Hansen, Walter Dorn, Martin Waelich and Eliot Higgins.
26 Interviews with Kristin Lund, Aderemi Adekoya and Walter Dorn.
27 Interviews with A Heather Coyne and Vincent Graf Narbel.
28 ICRC (2021a).
29 Pauwels (2021). Propaganda, disinformation and hate speech are covered by "data scraping".
30 Interview with Gary Brown.

BOX 2

Sensors embedded in accessible technologies

As well as enabling real-time communications and access to radio, the Internet and more, smartphones and other mobile phones incorporate a range of sensors, in particular camera technology. These sensors can help to gather evidence of certain activities and to share these data more widely, such as on social media.

While mobile phone penetration varies by region and country, this technology is available to a wide range of people and its use continues to expand. This has an impact on civilians, some of whom increasingly play a role in ceasefire monitoring and can help monitor certain activities taking place in private spaces, which may be harder to access using other technologies.[31]

However, while the use of civil society monitors can help data collection, this type of monitoring is only remote for the monitors – not the civilians themselves – and this can be to the detriment of the security of those civilians. The issues regarding the use of technology by civil society is discussed further in Chapter 3.

Table 3. Technologies enabling analysis

TECHNOLOGY	DESCRIPTION
Artificial intelligence (AI)	AI is made up of algorithms that use a logic-based approach to automate tasks; AI can therefore aid with data collection, the synthesis of information or its analysis, including pattern recognition, problem-solving and the provision of decision-making support.
Data fusion	Data fusion can enable the mapping, visualisation and reporting of vast amounts of different types of data.

31 Interview with Mark Lattimer.

BOX 3

Combining technologies

Technologies can be combined to work together or to leverage each other's advantages. For example, several sensors, such as motion sensors and cameras, can be employed in combination, with the data then being triangulated and merged to form a more detailed perspective. In a similar sense, technologies can be used jointly; for example, advanced binoculars, satellite imagery and data scraping could be used in combination in order to obtain a range of different information.

Several ongoing projects demonstrate the possibilities of combining AI with various data acquisition technologies, such as in various types of sensors, satellites, aerial platforms, and media platforms. One example is the pairing of UAVs and thermal cameras by the International Committee of the Red Cross (ICRC) to identify heat anomalies on the ground. AI is then employed to help analyse the data and identify if any of these anomalies are evidence of landmines.[32] The same approach is undertaken to analyse videos and images to identify cluster munitions.[33] Another example is from policing, where a company is combining UAVs, cameras, acoustic sensors and AI to determine the location of gunshots and provide a remote video feed of an ongoing situation.[34]

Table 4. Communications technology

TECHNOLOGY	DESCRIPTION
Information management	Communications technology is an essential enabling technology for ceasefire monitoring and verification, allowing communication between monitors, between monitors and the conflict parties, between the conflict parties, or between civil society and the monitors.

32 ICRC (2020); Interview with anonymous expert A.
33 Interview with Adam Harvey.
34 Coxworth (2021).

BOX 4

Creative communication: Whiteflag protocol

An example of a communications platform is the Whiteflag protocol. Originally built for deconfliction purposes, this communications platform uses blockchain, a technology that enables an immutable record of messages exchanged and thus transparency on these exchanges.[35]

Whiteflag messages are pre-defined; this helps ensure that what is sent is interpreted in the same way by all. Furthermore, due to the small size of the messages, a good Internet connection is not necessary to ensure the usability of the system.[36] However, it should be noted that at present Whiteflag is not a ready-made application, requiring a certain level of technical skill to be built.

2.3 MAPPING TECHNOLOGIES TO THE CEASEFIRE ACTIVITIES

Table 5 maps the technologies against the ceasefire activities, based on the technical abilities of a technology to acquire the relevant data. The number of tick marks represents the extent to which a technology is adapted to helping monitor or verify an activity – the greater the number of tick marks, the more adapted the technology. This signals both the fact that this technology has already been used to help monitor or verify the relevant activity or would have the ability to do so. This mapping is nonetheless indicative; depending on the specific activities encompassed within an agreement, the appropriateness of the technology for a specific activity may differ. Furthermore, tick marks have not been assigned to analysis and communications technologies, as these do not help to directly monitor or verify an activity, unlike the data acquisition technologies; rather, they support the data acquisition technologies and overall ceasefire monitoring and verification.

35 Interviews with Vincent Graf Narbel and Timo Schless; Whiteflag (n.d.).
36 Interview with Timo Schless; Whiteflag (n.d.).

Table 5. Technologies mapped against the ceasefire activities

		Weapons and ammunition	Troops and combatants	Non-lethal hostile activity	Protection of civilians	Infrastructure	Humanitarian assistance	Peacekeeping duties	Prisoners and hostages	Propaganda, hate speech and other hostile media
Data acquisition	Accoustic sensors	✓✓	-	✓	-	-	-	-	-	-
	Cameras	✓✓	✓✓	✓✓	✓	✓✓	✓	✓	✓	-
	Infrasound sensors	✓✓	-	-	-	-	-	-	-	-
	Motion sensors	✓	✓	✓✓	-	-	-	-	-	-
	Radars	✓✓	✓✓	✓✓	✓	✓✓	✓✓	✓✓	✓	-
	Satellites	✓✓	✓	✓	✓	✓✓✓	✓	✓	✓	-
	Seismic sensors	✓	✓	✓	-	-	-	-	-	-
	Aerial platforms	✓✓✓	✓✓	✓✓	✓	✓✓	✓✓	✓✓	✓	-
	UAVs	✓✓✓	✓✓	✓✓	✓	✓✓	✓✓	✓✓	✓	-
	Crowdsourcing	✓	✓	✓	✓	✓	✓	✓	✓	✓✓✓
	Data scraping	✓	✓	✓	✓	✓	✓	✓	✓	✓✓✓
	Advanced binoculars	✓	✓	✓	✓	✓	✓	✓	✓	-
	Biometrics	-	✓	-	-	-	-	-	-	-
	Cyber monitoring	✓	-	✓✓	-	✓✓	-	-	-	-
	RFID	✓	-	-	-	-	-	-	-	-
Analysis	Artificial intelligence									
	Data fusion									
Communications										

CROSS-CUTTING TECHNOLOGIES

Key: ✓✓✓ = technology very well adapted for this activity; ✓✓ = technology moderately adapted, may not be suitable for all specific areas falling under this activity; ✓ = technology has limited and/or specific areas of applicability within this activity; - = technology not suited for this activity.

The overview of technologies and subsequent mapping demonstrates the following.

- Most technologies are better suited to monitoring or verifying larger-scale activities, as opposed to activities of a smaller-scale or that take place in private, rather than in the public sphere.
- Technologies face certain common limitations and challenges. For example, hardware is likely to face operational challenges in difficult weather or terrain, although the type of weather conditions causing problems will differ according to the technology. Hardware is also vulnerable to physical action taken against it; for example, it can be targeted and shot at. Software is similarly vulnerable to targeting and can be jammed or hacked. Finally, most technologies require a certain level of technical ability to use or maintain them.
- While none of the technologies presented is well-suited to help with all of the identified ceasefire activities, technologies have been shown to complement and work with each other.[37] However, using multiple technologies also raises the need to ensure that they can work together in an integrated manner.[38]
- Technology can be used independently of whether it is monitoring and reporting incidents; verifying a reported incident and qualifying it, if applicable, as a violation; or, conversely, as a way to help resolve incidents, de-escalate situations that might lead or have led to a breach of a ceasefire, or map progress made by conflict parties towards a peace agreement.
- Regarding data acquisition technologies specifically, the indiscriminate way in which data is collected means that these data may go beyond the mandate of the monitoring and verification mechanism.

37 Interview with Piero Boccardo; validation workshop discussions.
38 Validation workshop discussions.

Liberia, 2018 - A member of the Chinese Formed Police Unit (FPU) deployed with UNMIL operates a drone with a video camera during a long range patrol to Tubmanburg, destination of the last long range patrol the contingent is conducting before withdrawal.
Credit: UN Photo/ John Isaac

3. Guiding considerations for the use of technology in remote ceasefire monitoring and verification

The use of technology in a ceasefire context does not occur in a vacuum – there are multiple other aspects that should be considered. This chapter therefore outlines 12 considerations regarding the use of technology for remote ceasefire monitoring and verification. These should be taken into account alongside the limitations and challenges of individual technologies outlined in Chapter 2 as well as the specific mandate of any ceasefire monitoring and verification mechanism. The considerations are presented alongside a set of questions to illustrate how they could be thought about in practice. As the considerations below demonstrate, technology is a tool that can help with remote ceasefire monitoring and verification, but it is not a solution in itself.[39]

Figure 2 provides an overview of the guiding considerations; many of these are closely tied to one another and have areas of overlap. Therefore, while the considerations are presented sequentially here, this does not imply that the considerations should be assessed in this specific order.

Figure 2. Overview of the guiding considerations

SUITABILITY	DEPLOYABILITY	GOVERNANCE
• Initial considerations • Contextual knowledge • Implications of technology use • Limitations of technology	• Practical considerations • Data management • Cost considerations • Level of technological knowledge	• Trust in technology • Security of technology and data • Ethics and privacy • Data sharing

3.1 SUITABILITY

Considerations under this section consider the suitability of using technology to aid with ceasefire monitoring and verification. This includes assessing issues such as whether the mandate allows for the use of technology, whether certain technologies are appropriate for use given local circumstances, and considering (unintended) implications of technology use.

3.1.1 Initial considerations

The existence of a relevant technology does not necessarily imply that it should be used, or even can be used. Comprehensive answers to the following questions would prove beneficial when first considering the use of technology:

39 Interviews with Thomas Simpson and Sanjana Hottatuwa.

- Why are one or several technologies needed?
- What would be the purpose of the technologies?
- To what extent does the use of the technologies fit with the ceasefire mechanisms?

Questions regarding the acquisition of technology include deciding between off-the-shelf products, which have not been built for ceasefire monitoring and verification purposes, versus a custom technology. Considerations regarding off-the-shelf products include, for example, the business model of the proprietary organisation and any possible neutrality or impartiality issues.[40] However, if a custom technology is selected, considerations include the timeline for this technology to be prepared, tested, and operationalised, as well as whether and how to include conflict parties in its development.[41]

Furthermore, technology should only collect the data necessary "to minimise vulnerability and potential harm".[42] Indeed, if technology is perceived to gather information beyond the scope of the mission's mandate, then this could become a security risk for monitors and other relevant stakeholders locally. Similarly, if excess data is collected, procedures will be needed to explain why this was the case and to ensure that such information is managed appropriately.[43]

Overall, it is important to define from the start the role that technology is meant to play and the objectives it is meant to fulfil under the ceasefire mechanism as this can help frame the purpose of technology use and also which specific technologies could be employed: will technology be used to monitor and verify incidents, map progress, and ensure better security and safety of monitors? Or will it be used as a way to build confidence between the conflict parties, such as through dialogue regarding the technology to be employed?

Good knowledge of the limitations, challenges and benefits of technology can help with these initial considerations. Early involvement of technology experts, for example as part of the discussions around ceasefire implementation modalities or even as part of the negotiations on a ceasefire depending on the context, and close communication and cooperation between technology and ceasefire experts can help address these initial questions and select the most relevant technologies, if any.[44]

40 Interview with Annika Hansen.
41 Interviews with Tim Schless and Martin Waehlisch.
42 United Nations Peacekeeping (2020, 7).
43 Correspondance with Georg Stein.
44 Interviews with Thomas Simpson and John Jaeger.

Illustrative questions

- *What is the purpose of using one or several technologies? Which specific objectives under the mandate of a ceasefire would technology serve best?*
- *What types of activity is the mission monitoring and verifying? What technology, if any, can best help obtain or analyse this information?*
- *Do the selected technologies prioritise certain types of activity or data over others? What impact could this have on the cooperation between the parties, on the situation on the ground or on the functioning of the ceasefire regime, if any?*

3.1.2 Contextual knowledge

The fact that a technology has been successfully used in one setting does not imply that it will work as successfully in another location. For example, mobile phones were considered for use in Myanmar's Kachin state to improve the ceasefire monitoring efforts and provide an easier and faster solution for the civil society monitors, as has been the case in other contexts. However, an assessment demonstrated that the use of mobile technology would place the civil society monitors in greater personal danger, in part due to issues around limited data security and digital literacy; as such, the use of this technology was not put in place.[45]

Furthermore, technology as a whole or specific technologies may not be accepted politically by the conflict parties or be appropriate for use. Acceptability may be diminished due to suspicion around the technology's purpose and scope; local experiences may also affect the views of conflict parties on technology to aid remote ceasefire monitoring and verification – for example, if the same technology has also been used to perpetuate violence by conflict parties (see Box 5).[46]

45 Interview with Joseph Guay; Rudnick et al. (2020).

46 Interviews with Laura Walker McDonald, Margaux Pinaud and anonymous expert G; Verjee (2019).

BOX 5

Aerial platforms as weapon systems versus monitoring tools

The acceptability of aerial platforms may be diminished by their use to fulfil different functions. If an aerial platform, such as UAVs or helicopters, has been used by conflict parties as a weapon, its use by the ceasefire mission as a monitoring tool can be misperceived, or it may be confused as belonging to one or several of the conflict parties, as was the case for the OSCE SMM to Ukraine with regard to UAVs.[47] To work around this issue, the OSCE SMM to Ukraine took mitigation measures, such as the placing of transponders on the UAVs and custom painting them. However, these were not infallible, and the mission's UAVs were still targeted.[48]

Beyond acceptability of the technology, this consideration also encompasses knowledge of demography and linguistic and cultural factors. Knowledge on who has access to digital technologies and the homogeneity of this access across different sections of the population can help ensure that the analysis of the data collected avoids instances of bias, as specific groups such women, younger people, older people, and different socioeconomic groups such as marginalised communities and nomadic groups may have less access to technology.[49] For example, regarding data acquisition via crowdsourcing and data scraping, contextual knowledge involves understanding the degree of Internet penetration, digital literacy, smartphone ownership or access, levels of control or freedom over telecommunications, and what types of platforms are currently most used.[50] Knowledge on dialects, colloquial speech and language variations are also relevant.[51]

Illustrative questions

- *What technology may be more (or less) appropriate given local preferences and experiences?*
- *If conflict parties or the local population are encouraged to use a technology, is there equal access to the technology? Will all views be represented?*

3.1.3 Implications of technology use

Assessing the implications of using a technology or a combination of technologies can help understand the range of possible outcomes, from positive to negative, from intended to unintended. For example, a technology might help free human

47 Interviews with Alexander Hug and anonymous expert G.
48 Interview with Alexander Hug.
49 Interviews with Annika Hansen, Mallika Auplish, Laura Walker McDonald and anonymous expert J; Principles for Digital Development (n.d.).
50 Interviews with Annika Hansen, Mallika Auplish, Laura Walker McDonald and anonymous expert L; Verjee (2019).
51 Interviews with Timo Schless, John Jaeger and Aly Verjee.

monitors for other tasks, extend their ability to monitor hard-to-reach areas or even enable them to capture more incidents (or, conversely, more acts in accordance with the terms of the agreement), thus insuring a greater feeling of justice.

Beyond the ways in which technology could assist human monitors, it is also necessary to consider whether and how the use of technology could redefine or change acceptable behaviour by conflict parties. For example, it is unacceptable to target human monitors, but similar moral considerations may not exist when it comes to technological hardware or software, which may be more likely to be targeted thus impeding ceasefire monitoring and verification to a greater extent.

Additionally, conflict parties may also change their operational methods to evade technological monitoring, for example by avoiding undertaking certain actions during the time where satellites complete their fly over.[52] Another implication to consider is whether more technologically-led monitoring and verification could devalue conventional, human-based methods and lead to less value or trust being placed on reports by human monitors versus data captured via technology.[53] Finally, there is also a broader challenge around the potential over-reliance on technology, which can lead to "a false sense of informed decision-making".[54]

Illustrative questions

- *What advantages or challenges does the use of technology provide to the conflict parties? To the mission? To the monitors?*
- *What implications could the use of technology have for the conflict parties? For the mission? For the monitors? For other branches of the United Nations and regional organisations operating in the country or region?*

3.1.4 Limitations of technology

Technology is not a panacea, and expectations regarding a technology's limitations must be managed. For example, technology cannot monitor all activities encompassed by a ceasefire agreement to the same degree (see Table 5). This is particularly true regarding the protection of civilians in the private sphere (e.g., the prevention of sexual violence), which increasingly features in agreements.[55]

Limitations of technology may also include a lack of understanding of the local context, dialects, colloquial speech, and language variations used to avoid detection.[56] This demonstrates that technology can help complement and strengthen human efforts but cannot replace them. Sometimes, human presence is the best method to build trust, diffuse situations, reassure the local population,

52 Interviews with Govinda Clayton and anonymous experts E and L.
53 Validation workshop discussions.
54 DPPA & Centre for Humanitarian Dialogue (2019).
55 Interview with Aly Verjee.
56 Interviews with Timo Schless, John Jaeger and Aly Verjee.

and obtain information.[57] Understanding the limitations of technology can help ensure that it does not inadvertently increase tensions or create a basis for blame between conflict parties.

Illustrative questions

- *What are the known advantages and limitations or challenges of a technology? How can the limitations or challenges be mitigated?*
- *In what ways can technology and humans best complement each other in terms of the needs of the mission?*

3.2 DEPLOYABILITY

Considerations under deployability relate to the practical use of a technology. These include whether a mission has sufficient financial resources and technical know-how to enable the use of a technology, or whether a technology can be used given climate, terrain, and other similar considerations.

3.2.1 Practical considerations

Practical considerations reflect on the application of technology and the cessation of its use. For example, certain technologies may not be adapted to the specific weather conditions of the site of use, or they may require consistent access to electricity which may be logistically difficult. If several technologies are considered, ensuring their synergy in terms of the data collected or analysed is also crucial. Finally, practical considerations also include determining how a technology will cease to be used and removed following the end of the mission.

Illustrative questions

- *Can the technology be used in any type of environment? For example, can it operate without problem in cold and hot climates, rainy and cloudy weather, and urban and rural settings?*
- *Does the technology require any specific infrastructure to operate? For example, does the technology require Internet connectivity to work? Could these aspects hamper its effectiveness and use?*
- *Can the technology be imported into the region or country of focus?*

3.2.2 Data management

Beyond the technologies themselves, it is also important to consider how the data collected is to be managed. This includes considering the possibly very large data-storage requirements as well as the infrastructure required to transmit and

57 Interviews with a UN official and Eliot Higgins; Wittkowsky (2021).

process the data.[58] Within this, data-management considerations require planning the capacity and resources needed to analyse the data generated and to identify the relevant information. Beyond the analysis of the data, it is also necessary to define how the data will be used after it has been collected and analysed, and in particular to ensure that "surplus" data that goes beyond the purposes of the ceasefire monitoring and verification mandate is not used.

Finally, data-management considerations also include determining how technology will cease to be used and removed following the end of the mission and putting in place plans for the archival or destruction of data collected or analysed via the technology.

Illustrative questions

- *What data analysis infrastructure is needed to manage and process the data collected?*
- *How will data be stored and protected from (cyber)attacks?*
- *What assurances will be put in place to ensure that data not strictly relevant for ceasefire monitoring and verification will not be used?*

3.2.3 Cost considerations

There may be assumptions that employing technology is cheaper than human monitors and that using technology may reduce the number of personnel needed. Yet, this may not necessarily be the case. For example, use of technology may be more labour intensive than anticipated, with humans still needed to operate and maintain technology as well as to help conduct data analysis – perhaps only more remotely than previously.[59]

There are also several costs beyond the initial purchase or rental cost of a technology. Such costs may include maintenance requirements and the need to create a data-storage system. Furthermore, technology can wear out or may be destroyed, stolen or purposefully damaged, which will have an impact on costs.[60] These costs all need to be considered in order to ensure that the mission's financial resources are sufficient to ensure the full use of the selected technology.

Illustrative questions

- *What does the technology cost to purchase or rent, use, maintain, and upgrade? What is its expected lifetime? What are the replacement costs in case of loss or destruction?*
- *What is the cost of the personnel needed to operate or maintain the technology or to analyse the resulting data?*

58 Interviews with Jan Dirk Wegner, Andreas Wittkowsky, Valerie Sticher and anonymous expert H.

59 Interviews with Mark Lattimer, Gary Brown and anonymous experts D and F.

60 Interview with anonymous expert E.

3.2.4 Level of technological knowledge

Technologies vary in complexity, but even for low-tech options there should not be an assumption that monitors, conflict parties or the local population have knowledge of, for example, a technology's purposes or how it gathers or analyses data. Increasing the level of digital literacy among all relevant stakeholders is therefore important and is strongly tied to trust in the technology (see Section 3.3.1). For example, if there is a gap in specialist knowledge within the mission, there needs to be consideration of the need to train personnel or bring in people with the necessary skill set.[61]

Illustrative questions

- *Are any specialised personnel needed to operate or maintain the technology or to analyse the outputs obtained? If so, what type of expertise is needed, and can this knowledge be obtained?*
- *If conflict parties or the local population are encouraged to use a technology, do they have the necessary technological knowledge and skill to do so? Could discrepancies in digital literacy bring biases to the data?*
- *To what extent could the lack of technological knowledge among relevant stakeholders have an impact on the ability to use a technology?*

3.3 GOVERNANCE

This final set of considerations includes more abstract matters such as trust, ethics, and levels of information sharing. These go beyond practical issues relating to topics such as the mission's mandate or practical advantages or impediments of a specific technology.

3.3.1 Trust in technology

Trust in technology includes trust by all stakeholders (i.e., monitors, conflict parties, the local population, and other relevant actors) in the specific technologies, the data obtained, and the analysis produced. Trust needs to exist for a technology to be accepted and used to its full extent and to ensure that the use of technology does not cause a deterioration in relations, such as increased blame attribution,[62] or create the view that the ceasefire monitoring and verification mission is not impartial.[63] It should also be noted that conflict parties may discredit certain technologies as part of an effort to undermine ceasefire mechanisms, such as by alleging partiality or bias of certain technologies.

61 Interviews with Kristin Lund, Margaux Pinaud, Timo Schless, Andreas Wittkowsky, Aly Verjee and anonymous expert I.

62 Interview with Govinda Clayton.

63 Interview with Aderemi Adekoya.

Understanding a technology, how it works, and the benefits it brings for the conflict parties and wider population is intricately tied to trust. This understanding and trust can be fostered in several ways. One way is through communication, use cases, or demonstrations of technology.[64] Another is through transparency about the technology.[65] This includes sharing details regarding its risk assessment (e.g. how reliable it is, how interpretable the outputs are, any possible security risks, etc.) and data acquisition and use (e.g. how the data is stored and analysed, gathering only the necessary data to fulfil the mission's mandate).[66] Such measures can help ensure that the technologies proposed are neutral and objective and that measures have been put in place to prevent the technology from being manipulated.[67]

Illustrative questions

- *To what extent could trust-building between the conflict parties be eroded by the use of technology?*
- *To what extent do monitors, conflict parties and the local population understand and trust the technologies that are being considered for use?*
- *Does the technology proposed for use follow all objectivity, security, and ethical stipulations?*

3.3.2 Security of the technology and the data acquired

Security of technology by design is key to protecting not only the technology but also the data collected, analysed or communicated. Security breaches could have a widespread impact on the objectivity and reliability of the data used by the monitoring and verification mission as well as on individuals. Furthermore, the more technology is used, the greater the number of attack surfaces and therefore vulnerabilities. This can include actors leaking, illegally obtaining or tampering with the data, jamming or hacking systems, or launching cyberattacks.[68]

For each technology used, putting in place appropriate measures that take into account the various possibilities is therefore needed; for example, this could mean encrypting data on UAVs in case one crashes or is taken by a conflict party,[69] or having measures in place to identify disinformation attempts. If technologies are not properly secured and are misused or hampered in any way, this could also affect levels of trust, as noted above.[70]

64 Interviews with A Heather Coyne and Valerie Sticher.
65 Interview with anonymous expert L.
66 Interviews with Timo Schless, Camino Kavanagh, Mallika Auplish and Adam Harvey; communication with Georg Stein.
67 Interview with anonymous expert E.
68 Interviews with Joseph Guay and anonymous experts E and I.
69 Interview with anonymous expert A.
70 Interview with Govinda Clayton.

Illustrative questions

- *How might a technology be interfered with? What measures would need to be taken to prevent any security breaches?*
- *What might be the impacts, if any, if the technology is hacked, jammed, or taken by conflict parties or other actors?*
- *What measures can help ensure an appropriate level of digital hygiene by the relevant technology users?*

3.3.3 Ethics and privacy

When collected any data, the ethics and privacy of this information must be upheld. This includes the use of fail-safe mechanisms to secure personal data since, even if inadvertently gathered or shared, it may place individuals at risk through what is called the Mosaic effect. This effect refers to the possibility of connecting multiple pieces of data into a coherent whole in order to identify individuals.[71] A number of guiding documents already provide guidance on ethical and privacy issues and appropriate data-protection standards to consider.[72]

There are also security implications for civil society monitors and the local population that are closely tied to crowdsourcing and data-scraping approaches. In particular, the data gathered by civil society monitors can be used to identify and target them: personal devices such as smartphones gather enormous amounts of data while at the same time being very vulnerable to surveillance or even seizure, which could place civilians in harm's way.[73] There are ways to overcome such issues, such as using encrypted communication channels or virtual private networks, although this requires a minimum level of digital literacy and understanding of the potential risks tied to each technology.

Illustrative questions

- *Will the technology gather personal data? If yes, is the data collected, transmitted, handled, and stored in a secure manner? What measures will be taken to ensure that this personal data does not result in (unintended) harm?*
- *Who owns the data that is collected? What are their policies regarding that data? Who has access to the data?*
- *What might be the unintended harms of using data gathered by civil society monitors, such as via crowdsourcing?*

71 Interviews with Laura Walker McDonald and Joseph Guay.

72 These include, for example, *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, a joint report by ICRC and Privacy International, the *Strategy for the Digital Transformation of UN Peacekeeping*, which includes a list of principles to respect, the *Risk, Harms and Benefits Assessment Tool* by the United Nations Global Pulse, *The Principles for Digital Development*, which are living guidelines regarding the use of technology, and UNICEF's *Principles for Innovation and Technology in Development*.

73 Interviews with Vincent Graf Narbel, Mallika Auplish and anonymous expert F; Rudnick et al. (2020).

3.3.4 Data sharing

Dissemination of information can be part of the mission's mandate. This includes considering the parameters of what information will be shared, in what ways, to whom, and using which technological means (if any). Yet, the use of technology to acquire data means that much more information may be gathered and therefore disseminated, beyond information relevant to the mandate of the ceasefire monitoring and verification mechanisms (as discussed in Section 3.2.2).

Sharing of information on ceasefire monitoring and verification activities and findings can help engage the wider civil society in the ceasefire process.[74] It is nevertheless necessary to consider: whether the information may lead to unintended harm to individuals via the Mosaic effect;[75] whether the release of data may discredit the mission if it has not been properly verified;[76] whether the sharing of information may increase blame attribution and worsen the situation rather than improve it; and what impact this information may have on trust around the ceasefire agreement and the monitors.[77]

Illustrative questions

- To what extent should data and findings from the ceasefire monitoring and verification mission be shared, and to which stakeholders? What are the benefits and disadvantages of such an approach? If the data or findings are made public, is it possible to ensure that this will not result in (unintended) harm?
- How could relevant information be shared most effectively and inclusively?

74 Interviews with Margaux Pinaud and Aly Verjee.
75 Guay & Rudnick (2020).
76 Interview with Govinda Clayton.
77 Interviews with Govinda Clayton and Aly Verjee.

Ukraine, 2021 - An OSCE special monitoring mission monitoring officer flying an unmanned aerial vehicles (UAV).
Credit: OSCE/Athanasios Kaltsis

4. Conclusion

Technology already plays – and will continue to play – a role in ceasefire monitoring and verification, albeit to varying extents. While the technologies presented here each have advantages, they also all have their respective limitations and challenges. Furthermore, technology can be used to aid but cannot replace the necessary constant discussions between the conflict parties under the supervisory mechanisms established under the ceasefire, including monitoring and verification mechanisms. Notwithstanding the fact that technologies need to be agreed to by the parties before being used, this is not meant to put practitioners off the use of technology. Rather, it is meant to ensure a more deliberate use of technology, as prompted by the guiding considerations, in order to maximise the benefits of technology and limit potential problems. As such, five conclusions arise from this research.

Combining the strengths of both technology and humans can help balance out their respective limitations. Technology can act as a force multiplier, help to gather data across a range of activities, and help to analyse and make sense of this information. Human capabilities can help to build dialogue and trust and play a role in areas where technology is either unwelcome or inappropriate. Indeed, remote monitoring and verification using only technology is technically feasible, but not recommended: the human element cannot be completely removed.

Technology is flexible as to the intended function. Technology is flexible in that its use can be guided by the needs of the mission. For example, technologies can be used to either monitor or verify that incidents have not occurred, but they can equally be used for other purposes, such as to enable dialogue or map progress made by conflict parties.

Technologies used currently focus mainly on the monitoring task through the acquisition of data. Technology can blur the lines between monitoring, verification, analysis, and communications. However, technologies used currently are overall more oriented towards being used in monitoring than in verification tasks, as a greater proportion of technologies are used to acquire data. Indeed, verification appears to be less suited to being conducted remotely. Additionally, there has been a limited use of analytical technologies. This reflects the focus within ceasefires, peacekeeping, and other domains on keeping data synthesis and analysis as a human-led task, though this may shift in the future depending on the level of adoption of analytical technologies.

Layering of data acquisition technologies can leverage their respective benefits. All technologies have their limitations and challenges, and a single technology might not be able to provide sufficient information, communications, or analysis. Therefore, combining a range of technologies in a coherent manner could help leverage their benefits while offsetting their respective limitations. This can also

help improve confidence in the data collected and means there is redundancy across the data-collection system.

Technology can be a double-edged sword for trust. Trust in technology plays a very important role in terms of whether one or several technologies are used in a ceasefire context. While it is true that misused technologies can erode trust, technology could conversely be used to build trust. This can be achieved by enabling dialogue about the use of these technologies or demonstrating that incidents breaching the agreement – or actions indicating that the parties are abiding by the terms of the agreement – can and will be recorded objectively.

Based on the research and overall findings, examples of good practices to consider for the future have been identified. These could be undertaken by the United Nations and other relevant entities working within the ceasefire domain.

- **Promote the use of, and continuously refine and update, the guiding considerations** on the use of technology in remote ceasefire monitoring and verification, such as by encouraging the use of these considerations during mediation discussions.
- **Improve knowledge sharing.** This includes better data sharing between relevant stakeholders, such as the sharing of lessons learned regarding the use of technology in ceasefires, which could be achieved through a dedicated and regularly updated platform. It also includes the sharing of data enabling the use of certain technologies – such as the sharing of high-quality image or video data to train AI.
- **Encourage multi-stakeholder approaches** to bridge the gap between the technology, ceasefire, and local experts. This can be achieved by promoting the use of teams with mixed expertise.
- **Ensure a minimum level of technological knowledge,** such as through targeted training courses. This would mean that there is a common level of digital literacy among the mediators and monitors and greater familiarity with technologies more generally and in terms of what they can offer in support of ceasefire monitoring and verification mechanisms. Such training could also be expanded to include other relevant parties where possible.
- **Monitor the evolution of conflicts and related ceasefire agreements** to identify new areas where monitoring and verification may be required – such as in cyberspace – in order to understand and prepare for the future of ceasefire monitoring and verification.

Appendix A. Detailed overview of the technologies

This appendix provides a more detailed overview of the technologies described in Chapter 2, providing the following information for each technology:

- A brief description of the technology.
- Indicative examples of current or potential uses, including use cases in ceasefire and peacekeeping missions, as well as by other actors such as the private sector and non-governmental organisations.
- Overview of the main limitations and challenges, focusing on the technological aspects.

A.1 SENSORS

A.1.1 Acoustic sensors

Description and uses. Acoustic sensors detect and help locate the source of sounds, such as that of artillery.[78] There are two main types of acoustic sensor: passive and active. Unlike active sensors, passive sensors do not emit radio waves; the radio waves can become a target for conflict parties.[79] Acoustic sensors were used, albeit in a limited way, by the OSCE SMM to Ukraine to help identify the use of weapons. This technology is also used in other contexts, such as by some police agencies, to identify and geographically locate gunshot crimes (e.g., ShotSpotter).

Limitations and challenges. Acoustic sensors are easy to remove, making it hard to protect them, and they require a constant power source.[80] These types of sensors also identify all sounds, not just the types of sounds being monitored, such as gunfire, so a certain level of analysis is required to identify relevant sounds. Acoustic sensors are therefore quite a high-end technology, which requires specific know-how to place, operate and analyse the data collected.[81] Due to these challenges, the use of acoustic sensors as part of the OSCE SMM to Ukraine was limited.[82]

A.1.2 Cameras

Description and uses. Cameras include stationary cameras, such as CCTV, as well as non-stationary cameras, which can be placed on aerial platforms such as helicopters or aircraft, including UAVs.[83] The more advanced the camera – that is,

78 Interviews with Alexander Hug, Walter Dorn, Gary Brown, and anonymous experts E, G and H.
79 Interview with Alexander Hug.
80 Interviews with anonymous expert G and Alexander Hug.
81 Interview with anonymous expert G.
82 Interviews with Alexander Hug, Valerie Sticher and anonymous experts G and H.
83 Interviews with Alexander Hug, Walter Dorn, Andreas Wittkowsky, Ajay Sethi, Margaux Pinaud, Kristin Lund, a UN official and anonymous expert F, G and H.

with high resolution or with infrared or thermal capabilities – the more detailed and effective the information it is able to capture.[84] Inclusion of GPS capabilities in cameras also provides the time and location of an event, and is a particularly useful feature for non-stationary cameras.

Cameras have been used by several ceasefire missions, including the OSCE SMM to Ukraine and UNFICYP. In both instances, the cameras monitored the contact line (OSCE SMM to Ukraine) or buffer zone (UNFICYP).[85] In the case of the OSCE SMM to Ukraine, given the length of the contact line, cameras were primarily placed at specific hotspots.[86]

Limitations and challenges. Cameras have a limited field of vision; when incorporated on aerial platforms, cameras obtain data in a certain area at intervals or for a limited time period, depending on the flight pattern. Furthermore, image quality can vary.[87] Cameras can be hampered by problems such as poor weather conditions or foliage and can also be targeted by conflict parties to render them unusable, for example by shooting at them.[88] In terms of logistics, cameras need a power source to function and, particularly for stationary cameras, safe retrieval of data needs to be considered. For example, data could be retrieved in-person or sent in virtually, such as by satellite communication.[89]

A.1.3 Infrasound sensors

Description and uses. Infrasound sensors detect acoustic waves from 20 hertz and below, thus capturing sounds beyond the range detectable by acoustic sensors. While infrasound sensors have generally been employed within the natural sciences and to detect nuclear explosions, their use to detect the sound of smaller explosions stemming from conventional arms is now being explored. Prototypes show that these sensors would be able to detect explosions 25–40 kilometres away, however these have not yet been used, whether for ceasefire purposes or otherwise. These sensors are passive, meaning that they do not emit a radio signal and are thus not detectable by their radio waves.[90]

Limitations and challenges. The technology is still under development, but, based on the available information, these sensors cannot be used in environments which are too cold; the temperature must be at least –12 degrees Celsius. Weather conditions, such as snow and rain, can also affect the effectiveness of the sensor.[91] Further aspects may come to light as the technology matures and further testing is undertaken.

84 Interviews with Kristin Lund and anonymous experts D, G and E; ICRC (2020).
85 Interviews with Alexander Hug and Aderemi Adekoya.
86 Interviews with Alexander Hug and anonymous expert H.
87 Interview with anonymous expert H.
88 Interview with Alexander Hug.
89 Interviews with Alexander Hug and Andreas Wittkowsky.
90 Interview with Sebastian Schutte.
91 Interview with Sebastian Schutte.

A.1.4 Motion sensors

Description and uses. Motion sensors detect movement and can also be set-up to provide an alert on suspicious movements.[92] This technology has already seen limited use in ceasefire contexts. Notably, it has been incorporated in cameras used by UNFICYP to detect unauthorised movement in the buffer zone.[93]

Limitations and challenges. One of the limitations of motion sensors is that they can identify all movements; therefore, their use may be restricted to specific areas only, such as no-contact areas or near weapon cantonment areas. Motion sensors can also be targeted by conflict parties.

A.1.5 Radars

Description and uses. Radars use radio waves to detect stationary and moving objects and can show the velocity of an object, with the range of detection depending on the radar and the frequency band used.[94] Unlike other sensors, such as cameras, radars are not affected by weather conditions such as rain or fog, heat or cold, and they work in both night and daytime conditions. Radars have been used in ceasefire and peacekeeping contexts, such as within MINUSMA[95] and the United Nations Interim Force in Lebanon, to detect the use of military equipment or weapons on the ground, in the air and at sea.[96]

Limitations and challenges. Radars can only detect objects within their line of sight.[97] Radio waves can be hampered or interfered with by competing radio waves, foliage or conductive material along their path.[98] Furthermore, unlike data from cameras, radar requires specific expertise to interpret.[99]

A.1.6 Satellites

Description and uses. Satellites capture images of the ground from space. Satellite imagery is well suited to demonstrating the evolution of a situation over time, such as the moving of military equipment or changes to infrastructure, whereby cameras on satellites are used to take pictures from space.[100] If using images from commercial satellites, as is the case with data from the United Nations Satellite Centre (UNOSAT), the data is thus verifiable by third parties, which can increase trust in the activities captured by the satellites.[101]

---

92 Interviews with a UN official and anonymous expert E.
93 Dorn (2014).
94 Interview with Walter Dorn.
95 Security Council (2016).
96 Expert Panel on Technology and Innovation in UN Peacekeeping (2015).
97 Expert Panel on Technology and Innovation in UN Peacekeeping (2015).
98 Schneibel (2021).
99 Expert Panel on Technology and Innovation in UN Peacekeeping (2015).
100 Interviews with Kristin Lund, Alexander Hug, Annika Hansen, Patrick Loots, Walter Dorn, Camino Kavanagh, Piero Boccardo, Eliot Higgins, Ajay Sethi, Valerie Sticher, Aly Verjee, Joseph Guay, a UN official and anonymous experts A and C.
101 Interview with anonymous expert C.

This technology has been used in several contexts, including in support of ceasefire missions. For example, the OSCE SMM to Ukraine used satellite monitoring and UNOSAT has also provided support to several ceasefire missions.[102] Satellite imagery is a proven resource used by several other actors, such as by the open-source intelligence (OSINT) community (e.g., Bellingcat).[103] It can also be used to monitor conflicts and sanctions, and to identify arms movement or trafficking. A notable example of the use of satellite imagery in the humanitarian sector is that of the Satellite Sentinel Project, which identified, in 2011, new roads being built in the Abyei region on the border between Sudan and South Sudan through satellite data. This was corroborated by local eyewitness testimonies, helping to alert that armed forces were set to be deployed.[104]

Limitations and challenges. The limitations and challenges of satellite technology can be grouped into three categories:

- **Image resolution**: The resolution of satellite imagery will vary depending on the type of satellite capturing the data. While image resolution in the 30–50 centimetres range can provide sufficient detail, particularly for ceasefire monitoring, higher resolution images are more expensive than lower resolution ones.[105] Commercial satellite imagery varies in its resolution, although a United Nations mission can request UNOSAT support to procure the necessary data for the activities it wants to monitor.[106]
- **Scope of imagery**: Due to their fixed orbit, satellites operate cyclically, meaning that images taken over an area will be at a specific time each day.[107] This means that satellites cannot be manoeuvred over specific areas, and there may be areas without satellite cover.[108] Additionally, given the cyclical and predictable nature of the satellite trajectory, conflict parties could seek to avoid being captured violating the agreement during the fly-over, though this could change in the future (Box 7).[109] As with regular cameras, weather and geographical features can also hamper the effectiveness of satellites, in particular cloud cover[110] and areas with a lot of foliage such as trees.[111]
- **Data burden**: Satellite imagery results in a very high data burden and therefore large data-processing needs.[112]

102 Interview with anonymous expert C.
103 Interview with Eliot Higgins; Bellingcat (2015a) and (2015b).
104 Interview with Joseph Guay; Harvard Humanitarian Initiative (n.d.); Card & Baker (2014).
105 Interviews with Eliot Higgins, Piero Boccardo, Kristin Lund and anonymous experts A and C.
106 Interview with anonymous expert C.
107 Interviews with Piero Boccardo and anonymous expert C.
108 Interviews with Piero Boccardo and Jan Dirk Wegner.
109 Interviews with Alexander Hug and anonymous expert C.
110 Interviews with Alexander Hug; Jan Dirk Wegner, Joseph Guay, and anonymous expert A.
111 Interviews with Joseph Guay and anonymous expert A.
112 Interviews with Piero Boccardo and Jan Dirk Wegner.

BOX 6

Future of satellite imagery

The number of satellites, and in particular small satellites and satellite constellations (i.e., a group of satellites working together), is set to increase in coming years. This may improve the coverage and therefore frequency of satellite monitoring. Coverage will also improve through the increased use of radar satellites, which, unlike regular electro-optical satellites, can be used at night and are not hampered by cloud cover.[113]

A.1.7 Seismic sensors

Description and uses. Seismic sensors capture vibrations or ground motions, such as those caused by the movement of large military equipment such as tanks.[114] Some seismic sensors can also be used to identify vibrations caused by people.[115] While these sensors were considered by the OSCE SMM to Ukraine, they were ultimately not used.[116] There are no examples of this technology being used in a ceasefire monitoring and verification context.

Limitations and challenges. The type of ground that these sensors are placed on can have an impact on the extent of the vibrations they are able to pick up.[117] Additionally, depending on their sensitivity, seismic sensors may not be able to detect smaller vibrations, such as those from individuals walking, running or crawling.[118]

A.2 AERIAL PLATFORMS (WITH EMBEDDED SENSORS)

A.2.1 Aerial platforms (helicopters, airplanes, aerostats)

Description and uses. Traditional crewed and uncrewed aerial platforms include helicopters, airplanes and aerostats.[119] Cameras (including infrared or thermal cameras) and other sensors (such as radar and acoustic sensors) are usually integrated into aerial platforms. Helicopters, airplanes and aerostats have all been used in various ceasefire or peacekeeping missions to ensure that weapons are not used, that troops are not active or that infrastructure remains unchanged. For example, aerostats were used by MINUSMA and the United Nations Mul-

113 Interview with anonymous expert C; Schneibel (2021).
114 Interview with anonymous expert E.
115 Clemente et al. (2019); Mukhopadhyay et al. (2018).
116 Interview with Alexander Hug.
117 Lemer & Ywanna (2006).
118 Pakhomov (2004).
119 Interviews with Kristin Lund, Annika Hansen and Walter Dorn. Aerostats, which are balloons which use helium as opposed to fossil fuel, include tethered and untethered types. Tethered systems include "live" and "dead" tethers, depending on whether the aerostat is self-sustaining ("dead") or whether there is a continuous electrical supply ("live"). Beyond the aerostat itself, these platforms also comprise a ground anchor unit (if tethered) and a station for ground controllers.

tidimensional Integrated Stabilization Mission in the Central African Republic (MINUSCA).[120]

Limitations and challenges. These systems require sufficient space for take-off, landing and storage of the systems and their fuel. In the case of helicopters and airplanes, licensed on-board pilots are required. While aerostats do not have personnel on-board, they have limited mobility if tethered. Aerostats also need to be resupplied with helium regularly, which can be challenging logistically. Weather can also affect the use of these systems, in particular aerostats, which are more vulnerable to harsher weather, notably wind and rain. Furthermore, these systems are expensive,[121] requiring trained personnel to not only operate them but also regularly maintain and repair them.[122]

A.2.2 Uncrewed aerial vehicles

Description and uses. UAVs include fixed-wing and rotary-wing systems.[123] Both types of UAV can be embedded with a range of sensors such as cameras (including with thermal and infrared capabilities) or radar. Differences between fixed- and rotary-wing systems include the fact that large fixed-wing systems tend to be able to fly for longer but will generally require a take-off and landing strip. Smaller fixed-wing UAVs can be hand-launched. Rotary-wing system do not face the same take-off or landing considerations but have a more limited fly time than fixed-wing systems.[124] UAVs are used in a range of sectors, including peacekeeping and ceasefire monitoring. Long- and short-range UAVs have notably been used by MINUSCA, MINUSMA, the United Nations Mission in South Sudan[125] and the OSCE SMM to Ukraine. In the latter case, UAVs monitored for live exchanges of fire and the presence of weapons and any changes to their positioning.[126]

Limitations and challenges. The limitations and challenges of UAVs can be grouped into four categories:

- **Flight time**: Rotary-wing UAV flight time can be short (around 20–30 minutes), which can have an impact on the ability of the human operator to be sufficiently remote.[127] This affects the ability of such systems to provide continuous or static monitoring.[128]
- **Weather**: As with other aerial platforms, weather conditions can also affect the use of these systems, which may not function or may be vulnerable to

120 Interview with Walter Dorn; Security Council (2016); General Assembly (2019).
121 Interview with Kristin Lund.
122 Interview with Walter Dorn.
123 Interviews with Alexander Hug, Walter Dorn, Andreas Wittkowsky, Ajay Sethi, Valerie Sticher, a UN official and anonymous experts A, E, G and H.
124 Interview with anonymous expert H.
125 Druet (2021).
126 Interview with Alexander Hug; Buchanan et al. (2021).
127 Interview with Alexander Hug.
128 ICRC (2021b); Interview with Alexander Hug.

harsh weather conditions.

- **Operational needs**: Long-range UAVs may require more specialist personnel or contractors to operate them, compared to smaller and less complex systems, which can be operated without the need for specialist pilot licensing.[129]
- **System vulnerability**: An UAV can come down due either to a lack of power or to an attack (e.g., shot at, hacked or jammed electronically).[130] Ensuring that the data is secure and encrypted is therefore important should the UAV not be retrievable. If jammed, this can include ensuring that the UAV is programmed to return to base.[131]

A.3 MEDIA PLATFORMS

A.3.1 Crowdsourcing

Description and uses. Crowdsourcing enables the acquisition of data from a large number of people, using technologies discussed in Sections A.1 and A.2. Certain types of civilian monitoring can be classified as crowdsourcing, whereby civil society actively reports on incidents or shares information on events happening on the ground, such as through mobile phones or other Internet-connected platforms.[132] Conflict parties as well as other actors on the ground such as humanitarian actors can also report incidents. Crowdsourcing can provide monitors with real-time information, as well as information that builds on local knowledge.[133]

Crowdsourcing methods have been employed to varying extents in the ceasefire and peacekeeping domains. For example, the Ceasefire Centre for Civilian Rights established a civilian monitoring system in Iraq between 2014 and 2017 with Minority Rights Group International.[134] Civilian monitoring was also employed in Myanmar's Kachin State and in Nepal.[135] Other examples of crowdsourcing technologies and approaches include use in the humanitarian and electoral domains, such as by Humanitarian OpenStreetMap,[136] Ushahidi and eyeWitness.[137] For example, the Ushahidi platform was first used to monitor electoral violence in Kenya following the 2007 elections and has now evolved to crowdsourcing information on wider humanitarian issues. Information can be sent in multiple ways, such as through social media, SMS or email.[138]

129 Interview with Alexander Hug.
130 Interview with Alexander Hug; Tanner (2021); Giardullo et al. (2020)
131 Interview with Andreas Wittkowsky.
132 Interviews with Aly Verjee and anonymous expert F; Esberg & Mikulaschek (2021).
133 Puttick (2017).
134 Puttick (2017); Pinaud (2021).
135 Krause & Kamler (2022).;
136 Humanitarian OpenStreetMap Team (n.d-a); see for example: Humanitarian OpenStreetMap Team (n.d-b).
137 Hirblinger (2020).
138 Puttick (2017); Ushahidi (n.d.).

Limitations and challenges. The limitations and challenges of crowdsourcing can be grouped into five categories:

- **Linguistic and cultural knowledge**: Use of crowdsourced information requires good linguistic and cultural knowledge; while technology can help automate translation to a certain extent, it cannot replace an intrinsic understanding of linguistic nuances and cultural context.[139]
- **Accuracy of information**: The accuracy of crowdsourced information requires verification, as there is a possibility of misuse if users feed in fake or incorrect news.[140]
- **Risk of harm**: There is the risk that sensitive information about an incident or its victims could spread and create more harm.[141] This includes a risk to the safety and security of the local population or of civil society monitors collecting data.
- **Internet availability and accessibility**: Removal of Internet or banning of certain content or platforms can impede people from sharing information and also the retrieval of the data.[142] Furthermore, access to the Internet and other platforms that enable crowdsourcing may not be homogenous across the population; some sections of the population, such as the more disadvantaged or women, may not have equal access, and therefore their experiences may not be captured by the crowdsourced data.
- **Training**: Custom-made platforms are costly and are likely to require training to at minimum explain how to use them.[143] Roll-out of the training may be challenging, for example if it relies on a stable Internet connection, and people may revert to the use of more familiar and trusted platforms.[144]

A.3.2 Data scraping

Description and uses. Data scraping refers to the acquisition of data from news media (written press, television and radio) and social media to help understand the ongoing rhetoric.[145] For verbal data, this can involve the automatic transcription and even translation of information.[146] Regarding the scraping of data from social media, a range of ready-made media and social media monitoring services are already used by the OSINT community, such as CrowdTangle, Hixy, Zignal Labs, Meltwater, Talkwalker and TweetDeck, in addition to the possibility of creating a

139 Interview with Aly Verjee.
140 Puttick (2017); Interview with Govinda Clayton.
141 Puttick (2017).
142 Interview with anonymous expert L.
143 Interview with A Heather Coyne.
144 Interview with Sanjana Hattotuwa.
145 Interviews with Annika Hansen, Walter Dorn, Martin Waelich and Eliot Higgins.
146 Dorn & Giardullo (2021).

custom scraping and data-mining tool.[147]

Various forms of data scraping have been used in the humanitarian and peacebuilding domains, and to a lesser extent in the ceasefire domain as well. For example, radio monitoring was used by MINUSMA to "analyse radio data to detect hate speech, serving as an automated early-warning system for unrest".[148] The Innovation Cell of the United Nations Department of Political and Peacebuilding Affairs (DPPA) has also been developing an "AI-powered advanced media monitoring platform for television and radio content", which "automatically transcribes and translates spoken content on radio and television".[149] Another example involving social media is the monitoring of tweets. This is done, for example, by the Ceasefire Centre for Civilian Rights to identify human rights violations.[150] DPPA's Innovation Cell has also created a social media reporting tool, called Sparrow, which analyses Twitter data to help peacekeepers identify unfolding crises.[151]

Limitations and challenges. Some of the limitations and challenges affecting crowdsourcing also apply to data scraping, namely in relation to linguistic and cultural knowledge, Internet availability and accuracy of information. In addition, data scraping can only retrieve public data and not any information shared by private accounts or through encrypted messages such as WhatsApp or Telegram.[152] Therefore, data obtained via scraping can only represents a partial picture of ongoing rhetoric.

A.4 OTHER DATA ACQUISITION TECHNOLOGIES

A.4.1 Advanced binoculars

Description and uses. Advanced long-range binoculars are used by monitors to observe from a distance and include sensors such as cameras and infrared, enabling the recording of data during day and night.[153] This technology can help survey an area as well as ascertain the safety of a certain area before sending human monitors. Binoculars have notably been used as part of UNFICYP.

Limitations and challenges. While binoculars offer remote monitoring, they are not autonomous (i.e., a person is required to use them) and they can only enable the monitoring of small areas at a time. As such, binoculars are best suited to the monitoring of specific areas where other technologies, such as stationary cameras, cannot be used.

147 Interviews with Patrick Loots, Eliot Higgins and Joseph Guay.
148 United Nations (2021).
149 DPPA (2021b, 13).
150 Interview with Mark Lattimer.
151 DPPA (2021a).
152 Interview with anonymous expert J.
153 Interviews with Kristin Lund, Aderemi Adekoya and Walter Dorn.

A.4.2 Biometrics

Description and uses. Biometrics is a form of identification and authentication of an individual that relies on biological characteristics, such as fingerprints.[154] Biometrics have been used (or attempted to be used) by some humanitarian organisations, such as the United Nations High Commissioner for Refugee (UNHCR), which collects fingerprints and iris scans to verify the identity of refugees, as well as the World Food Programme, which has notably sought to use biometrics in Yemen to assist with food distribution.[155] This technology also tends to be used to help identify IDPs and refugees in situations of conflict, including as part of disarmament, demobilization and reintegration programmes.

Another form of biometrics that does not use biological characteristics is token-based biometrics. This is less invasive and "any data that is captured is stored on something the individual them self owns".[156] It is the method employed by the ICRC, in certain cases only, "to identify the deceased, facilitate reunification of separated families, or ensure the right people receive aid".[157] In the case of ceasefires, biometrics could for example be extended to help ascertain that the cantonment of troops is respected, or that there is no prohibited movement of troops and combatants.

Limitations and challenges. Biometrics concerns very personal and permanent individual information; if this information is stolen or lost, it could put the safety of the concerned individuals at risk. However, further research and development around the security of biometric data or the development of proprietary platforms could help overcome some of these limitations in the future.

A.4.3 Cyber monitoring

Description and uses. While the cyber dimension has not yet been included as part of a ceasefire agreement, cyberspace is increasingly used and is of increasing importance; indeed, developments taking place in cyberspace can have implications in the physical world, and vice versa.[158] For example, hate speech or propaganda spread through social media may cause an increase in tensions and lead to physical violence.

In this instance, cyber monitoring refers to the monitoring of attacks and operations targeting digital infrastructure, including the leaking, poisoning or stealing of data or targeting critical infrastructure.[159] However, one study has noted that the "monitoring and verification of offensive cyber operations is notoriously

154 Interviews with A Heather Coyne and Vincent Graf Narbel.
155 UNHCR (2015); Clausen (2021).
156 ICRC (2021a).
157 ICRC (2021a).
158 Interview with Sanjana Hattotuwa; Kane & Clayton (2021).
159 Pauwels (2021). Propaganda, disinformation and hate speech are covered within 'data scraping'.

difficult".[160] Generally, measures used by governments and companies currently to detect cyberattacks, such as through a computer security incident monitoring service, can help monitor for such events. However, these measures have never been used in a ceasefire context.[161]

Limitations and challenges. Verification of a cyberattack is likely to also involve attribution. However, attribution more generally is problematic, as identifying the party responsible for a cyber incident is extremely challenging.[162] The main challenge is obtaining an acceptable standard of proof, which is difficult since relevant data, such as IP addresses, are easy to spoof.

A.4.4 Radio-frequency identification

Description and uses. RFID technology helps track items by way of tags, enabling a mass-read out of inventory.[163] RFID tags can be categorised according to the frequency at which they operate and whether they are active or passive. Higher frequency tags can be read from a greater distance than low-frequency tags. Unlike active tags, passive tags do not have an internal power source and they have a longer lifespan. RFID tags are particularly used in logistics; however, there are no examples of this technology being used in a ceasefire monitoring and verification context, although RFID tags could be used to ensure that the cantonment of weapons is being respected according to the terms of the agreement.[164]

Limitations and challenges. The limitations and challenges of RFID can be grouped into two categories:

- **Trackable signal:** Unlike passive tags, active RFID tags broadcast a signal, which can be used to identify the location of the object that is tagged. This could be problematic as parties other than monitors could also track these signals, unless these tags are accompanied by a Faraday shield, which is used to block signals from active tags (and other systems using electro-magnetic waves).
- **Acceptability and trust:** The tagging of items such as weapons would require a high level of trust on the part of the conflict parties. This includes trust in the technology, trust in the monitors and trust that the weapons of other conflict parties are also being placed under similar scrutiny. Additionally, in a low-trust environment, conflict parties may not accept the placement of foreign technology on their weapons given the sensitive nature of this technology.[165]

160 Kane & Clayton (2021, 28).
161 Kane & Clayton (2021).
162 Interviews with Samuele Dominioni and anonymous expert K; Kane & Clayton (2021).
163 Interview with Gary Brown.
164 Interview with A Heather Coyne.
165 Interview with Alexander Hug.

A.5 ANALYSIS

A.5.1 Artificial intelligence

Description and uses. AI is made up of algorithms that use a logic-based approach to automate tasks. AI can therefore aid with data collection, the synthesis of information or its analysis, including pattern recognition, problem-solving or the provision of decision-making support. AI can also analyse a range of data types including images, videos,[166] and written and spoken language – which includes sentiment analysis (i.e., the ability to identify emotions or attitudes to a particular topic).[167] AI can, for example, be used for specific analytical tasks, such as the detection of manipulated images or videos that have been scraped from the web.[168] Subfields of AI include machine learning and deep learning, with the main difference being how these algorithms learn: deep learning does not involve as much human input when training compared to machine learning. While this technology has not yet been employed within ceasefire missions, DPPA's Innovation Cell have explored how AI could provide support, such as through a project monitoring the online and social media rhetoric surrounding the Nagorno-Karabakh conflict.[169]

Limitations and challenges. The limitations and challenges of AI can be grouped into three categories:

- **Understandability of conclusions**: AI – and particularly some types of AI, such as deep learning – can be problematic as it can be impossible to know how the AI came to a certain conclusion. As such, there has been a hesitancy to use AI for the analysis of information, as opposed to its synthesis.[170]
- **Data and the training of the algorithms**: Algorithms (other than deep learning) require training. Training of AI is time-consuming.[171] It also requires sufficiently high-quality data.[172] Biased training data is a risk, which could lead to inadvertent discrimination or false results.[173] However, there is generally a lack of data, which can hamper the use of AI.[174]
- **Algorithm ownership**: Privately developed algorithms raise questions regarding data security and confidentiality as well as the lack of transparency over the algorithms and their functions.[175]

166 Interviews with Adam Harvey, Vincent Graf Narbel and Joseph Guay.
167 Interview with Deeph Chana; DPPA & Centre for Humanitarian Dialogue (2019).
168 Interview with Joseph Guay; Esberg & Mikulaschek (2021).
169 DPPA (2021b).
170 Interview with Ajay Sethi.
171 DPPA & Centre for Humanitarian Dialogue (2019).
172 Interviews with Jan Dirk Wegner, Adam Harvey and anonymous expert A.
173 DPPA & Centre for Humanitarian Dialogue (2019).
174 Interview with Martin Waehlisch.
175 DPPA & Centre for Humanitarian Dialogue (2019).

A.5.2 Data fusion

Description and uses. Data fusion can enable data mapping, data visualisation and reporting of vast amounts of different types of data. Data fusion can take different forms depending on what data is collected and what monitors want to know from the data. Subsets of data-fusion technologies include, for example, geographic information systems (GIS), which use geotagged data to map various types of information geographically. Examples of data fusion and visualization technologies include IBM i2 iBase, which has been used by the All Sources Information Fusion Unit in MINUSMA;[176] ActivityInfo, a service which offers information-management solutions;[177] and the United Nations' own proprietary technology, Situation Awareness Geospatial Enterprise (SAGE).[178] Technologies such as GIS and SAGE have already been used in ceasefire and peacekeeping context.[179] For example, the OSCE SMM to Ukraine, has made use of enterprise GIS.[180]

Limitations and challenges. Mirroring the issues outlined for AI technologies above, the limitations and challenges of data fusion can be grouped into two categories: quality of data and ownership of the tool. Regarding the quality of the data, the more consistent and the more complete the data, the better it will be for data fusion. For example, geotagged data is more useful than non-geotagged information.

A.6 COMMUNICATIONS

Description and uses. Communications technology is an essential enabling technology for ceasefire monitoring and verification. This can include communication between the monitors, between the monitors and the conflict parties, between the conflict parties, or between civil society and the monitors. Communications technology can be used to coordinate activities, share information and help build trust. Different technologies exist. Video conferencing and mobile phone technology are established technologies.[181] Other custom-made technologies are also possible. For example, a platform is being developed by Hala Systems in coordination with the United Nations Mission to support the Hudaydah Agreement (UNMHA) in Yemen to enable communications between the conflict parties and to help them address incidents collaboratively. This type of platform uses these communications to help monitor commitments to the agreement as well as track progress in relations between conflict parties.[182]

176 Druet (2021).
177 Karlsrud (2014).
178 Interview with John Karlsud; Duursma & Karlsrud (2019).
179 DPPA & Centre for Humanitarian Dialogue (2019); United Nations Peacekeeping (2020).
180 Dorn & Giardullo (2021).
181 Interviews with Camino Kavanagh, Margaux Pinaud, Joseph Guay and anonymous expert G.
182 Interviews with A Heather Coyne and John Jaeger.

Limitations and challenges. Different communications platforms will face different problems. However, one overarching challenge is ensuring the security of the information shared and received; ensuring proper cybersecurity is therefore a core requirement.

Appendix B. Research participants

We are grateful for the following experts who took part in the research interviews and for the information they contributed (Table 6). We also thank the experts who took part in the validation workshop.

Table 6 List of interviewed experts

Name	Affiliation	Date of interview
Mr Aderemi Adekoya	United Nations	7 October 2021
Ms Mallika Auplish	Vital Strategies	29 October 2021
Prof. Piero Boccardo	Polytechnic of Turin	26 October 2021
Prof. Gary Brown	National Defense University, United States	16 November 2021
Prof. Deeph Chana	Imperial College London	8 December 2021
Dr Govinda Clayton	Center for Security Studies (CSS) at ETH Zürich	24 September 2021
Ms A. Heather Coyne	United Nations	21 September 2021
Dr Samuele Dominioni	UNIDIR	21 December 2021
Prof. Walter Dorn	Royal Military College of Canada (RMC)	15 October 2021
Mr Joseph Guay	Twitter	14 December 2021
Dr Annika Hansen	Center for International Peace Operations (ZIF)	11 October 2021
Mr Adam Harvey	Independent researcher	12 November 2021
Dr Sanjana Hattotuwa	ICT4Peace Foundation	16 November 2021
Mr Eliot Higgins	Bellingcat	8 November 2021
Mr Alexander Hug	International Commission on Missing Persons (ICMP)	1 October 2021
Mr John Jaeger	Hala Systems, Inc.	15 October 2021
Dr John Karlsrud	Norwegian Institute of International Affairs (NUPI)	28 October 2021
Dr Camino Kavanagh	King's College London	19 October 2021
Mr Mark Lattimer	Ceasefire Centre for Civilian Rights	13 October 2021
Mr Patrick Loots	United Nations	11 October 2021
Maj. Gen. Kristin Lund	Former Force Commander of UNFICYP–	23 September 2021
Mr Vincent Graf Narbel	ICRC	6 December 2021
Dr Margaux Pinaud	Centre on Conflict, Development and Peacebuilding (CCDP)	10 November 2021
Mr Timo Schless	Whiteflag Foundation	17 December 2021
Dr Sebastian Schutte	Peace Research Institute Oslo (PRIO)	26 October 2021
Mr Ajay Sethi	United Nations	9 November 2021
Mr Thomas Simpson	Hala Systems, Inc.	6 October 2021
Dr Valerie Sticher	Center for Security Studies (CSS) at ETH Zürich	3 November 2021
Mr Aly Verjee	United States Institute of Peace (USIP)	2 December 2021
Dr Martin Waehlisch	United Nations	27 January 2022
Ms Laura Walker McDonald	ICRC	15 December 2021

Prof. Jan Dirk Wegner	ETH Zürich	19 November 2021
Dr Andreas Wittkowsky	Center for International Peace Operations (ZIF)	4 November 2021
-	Arms expert, United Nations	20 October 2021
-	United Nations official	17 November 2021
Anonymous expert A	-	23 November 2021
Anonymous expert B	-	19 November 2021
Anonymous expert C	-	13 December 2021
Anonymous expert D	-	19 October 2021
Anonymous expert E	-	6 October 2021
Anonymous expert F	-	13 October 2021
Anonymous expert G	-	15 October 2021
Anonymous expert H	-	28 October 2021
Anonymous expert I	-	27 October 2021
Anonymous expert J	-	16 November 2021
Anonymous expert K	-	21 December 2021
Anonymous expert L	-	25 January 2022

References

Bara, Corinne, Govinda Clayton & Siri Aas Rustad. 2021. "Understanding Ceasefires." *International Peacekeeping*, 28 (3): 329-340. As of 23 June 2021: https://www.tandfonline.com/doi/full/10.1080/13533312.2021.1926236?scroll=top&needAccess=true

Bellingcat. 2015a. *Russia's Path(s) to War: A bellingcat Investigation.* As of 18 March 2022: https://www.bellingcat.com/app/uploads/2015/09/russia_s_path_s__to_war.pdf

Bellingcat. 2015b. *Forensic Analysis of Satellite Images Released by the Russian Ministry of Defense: A bellingcat Investigation*. As of 18 March 2022: https://www.bellingcat.com/app/uploads/2015/05/Forensic_analysis_of_satellite_images_EN.pdf

Buchanan, Cate, Govinda Clayton & Alexander Ramsbotham. 2021. *Ceasefire monitoring: developments and complexities*. Accord Spotlight. UK: Conciliation Resources and Political Settlements Research Programme. As of 24 March 2022: https://rc-services-assets.s3.eu-west-1.amazonaws.com/s3fs-public/Ceasefire_monitoring_Developments_and_complexities.pdf

Card, Brittany L. & Isaac L. Baker. 2014. "GRID: A Methodology Integrating Witness Testimony and Satellite Imagery Analysis for Documenting Alleged Mass Atrocities." *Genocide Studies and Prevention: An International Journal*, 8(3): 49-61. DOI: http://dx.doi.org/10.5038/1911-9933.8.3.5

Clausen, Maria-Louise. 2021. *Piloting Humanitarian Biometrics in Yemen*. PRIO Middle East Centre Mideast Policy Brief 01. As of 13 April 2022: https://reliefweb.int/sites/reliefweb.int/files/resources/Clausen%20-%20Piloting%20Humanitarian%20Biometrics%20in%20Yemen%2C%20MidEast%20Policy%20Brief%201-2021.pdf

Clemente, Jose, WenZhan Song, Maria Valero, Fangyu Li & Xiangyang Li. 2019. "Indoor Person Identification and Fall Detection through Non-Intrusive Floor Seismic Sensing." *IEEE International Conference on Smart Computing (SMARTCOMP),* pp. 417-424. DOI: http://doi.org/10.1109/SMARTCOMP.2019.00081

Coxworth, Ben. 2021. "New policing system will send drones to the source of gunshots." *New Atlas,* 21 December. As of 22 March 2022: https://newatlas.com/drones/shotspotter-airobotics-drones-gunshots/

Dorn, A. Walter & Cono Giardullo. 2021. Analysis for Peace: The Evolving Data Tools of UN and OSCE Field Operations. Security and Human Rights, 31(1-4), 90-101. doi: https://doi.org/10.1163/18750230-31010001

Dorn, Walter A. 2014. "Electronic Eyes on the Green Line: Surveillance by the United Nations Peacekeeping Force in Cyprus." *Intelligence & National Security*, 29:2, 184-207. As of 16 March 2022: https://www.tandfonline.com/doi/abs/10.1080/02684527.2013.834216

Dorn, Walter A. 2016. "Smart Peacekeeping: Toward Tech-Enabled UN Operations." *Providing for Peacekeeping* No. 13. As of 18 March 2022: www.ipinst.org/wp-content/uploads/2016/07/1607_Smart-Peacekeeping.pdf

DPPA & Centre for Humanitarian Dialogue. 2019. *Digital technologies and mediation in armed conflict*. As of 22 March 2022: https://peacemaker.un.org/sites/peacemaker.un.org/files/DigitalToolkitReport.pdf

DPPA. 2021a. *Multi-Year Appeal Quarterly Report January-March 2021*. As of 22 March 2022: https://dppa.un.org/sites/default/files/6209_unny_quarterly_report_final_0.pdf

DPPA. 2021b. *Multi-Year Appeal Quarterly Report April--June 2021*. As of 22 March 2022: https://dppa.un.org/sites/default/files/6298_unny_quaterly_report2_april_highres.pdf

Druet, Dirk. 2021. *Enhancing the use of digital technology for integrated situational awareness and peacekeeping-intelligence*. Thematic Research Paper for the DPO Peacekeeping Technology Strategy. As of 18 March 2022: https://peacekeeping.un.org/sites/default/files/20210430_-_sa-pki_technologies_research_brief_final_clean.pdf

Duursma, Allard & John Karlsrud. 2019. "Predictive Peacekeeping: Strengthening Predictive Analysis in UN Peace Operations." *Stability: International Journal of Security and Development*, 8(1), p.1. http://doi.org/10.5334/sta.663

Ermochenko, Alexander & Pavel Polityuk. 2021. "Separatists end blockade of hotel housing conflict monitors in eastern Ukraine." *Reuters*, 18 October. As of 16 March 2022: https://www.reuters.com/world/europe/osce-says-rebels-eastern-ukraine-holding-its-monitors-prisoner-hotel-2021-10-18/

Esberg, Jane & Christoph Mikulaschek. 2021. *Digital technologies, peace and security: challenges and opportunities for United Nations Peace Operations*. As of 18 March 2022: https://peacekeeping.un.org/sites/default/files/esberg_and_mikulaschek_-_conflict_peace_and_digital_technologies_-_v3_210825.pdf

Expert Panel on Technology and Innovation in UN Peacekeeping. 2015. *Performance peacekeeping: Final report of the Expert Panel on Technology and Innovation in UN Peacekeeping*. As of 16 March 2022: https://peacekeeping.un.org/sites/default/files/performance-peacekeeping_expert-panel-on-technology-and-innovation_report_2015.pdf

General Assembly. 2019. "Budget for the United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic for the period from 1 July 2019 to 30 June 2020." A/73/772. As of 18 March 2022: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/056/62/pdf/N1905662.pdf?OpenElement

General Assembly. 2020. “Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation.” A/74/821. As of 16 March 2022: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/51/PDF/N2010251.pdf?OpenElement

Giardullo, Cono, Walter Dorn & Danielle Stodilka. 2020. “Technological Innovation in the OSCE: The Special Monitoring Mission in Ukraine.” In: IFSH (ed.), *OSCE Yearbook 2019*, Baden-Baden 2020, pp. 119-137.

Guay, Joseph & Lisa Rudnick. 2020. “Open Source Investigations: Understanding Digital Threats, Risks, and Harms.” In S. Dubberley, A. Koenig, and D. Murray (eds). *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*. Oxford University Press.

Harvard Humanitarian Initiative. N.d. *Making the world a witness: Report on the pilot phase, December 2010 - June 2012.* Satellite Sentinel Project.

Hirblinger, Andreas T. 2020. *Digital Inclusion in Peacemaking: A Strategic Perspective*. The Centre on Conflict, Development and Peacebuilding, CCDP Working Paper 14.

Humanitarian OpenStreetMap Team. N.d-a. “What we do.” As of 18 March 2022: https://www.hotosm.org/what-we-do

Humanitarian OpenStreetMap Team. N.d-b. “Refugee Response: South Sudan and Syria.” As of 18 March 2022: https://www.hotosm.org/projects/urban_innovations_crowdsourcing_non-camp_refugee_data

ICRC. 2020. “Drones, infrared cameras and AI join the search for mines.” *ICRC Inspired*, 16 June. As of 16 March 2022: https://blogs.icrc.org/inspired/2020/06/16/drones-infrared-cameras-mines/

ICRC. 2021a. “The Biometrics Minefield.” *ICRC Inspired*, 26 February. As of 22 March 2022: https://blogs.icrc.org/inspired/2021/02/26/the-biometrics-minefield/

ICRC. 2021b. “Drones, Data and Humanitarian Action.” *ICRC Inspired*, 27 April. As of 18 March 2022: https://blogs.icrc.org/inspired/2021/04/27/drones-data-and-humanitarian-action/

Kane, Sean & Govinda Clayton. 2021. *Cyber Ceasefires: Incorporating Restraints on Offensive Cyber Operations in Agreements to Stop Armed Conflict*. CSS Mediation Resources. As of 22 March 2022: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/MediationResources_CyberCeasefires.pdf

Karlsrud, John. 2014. “Peacekeeping 4.0: Harnessing the Potential of Big Data, Social Media, and Cyber Technologies.” In: Kremer JF., Müller B. (eds) *Cyberspace and International Relations*. Springer: Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37481-4_9

Krause, Jana & Erin Kamler. 2022. "Ceasefires and Civilian Protection Monitoring in Myanmar." *Global Studies Quarterly*, 2 (1). As of 13 April 2022: https://doi.org/10.1093/isagsq/ksac005

Lemer, Alain & Frederique Ywanne. 2006. Acoustic/Seismic Ground Sensors for Detection, Localization and Classification on the Battlefield. In *Battlefield Acoustic Sensing for ISR Applications* (pp. 17-1 – 17-12). Meeting Proceedings RTO-MP-SET-107, Paper 17.

Mukhopadhyay, Bodhibrata, Sahil Anchal & Subrat Kar. 2018. "Person Identification using Seismic Signals generated from Footfalls." *ArXiv*. As of 18 March 2022: https://arxiv.org/pdf/1809.08783.pdf

Nicols, Michelle. 2016. "Syria conditions make it hard to deploy U.N. ceasefire monitors - U.N. chief." *Reuters, 18 February.* As of 23 June 2021: https://www.reuters.com/article/mideast-crisis-syria-un-idINKCN0VR2J3

Pakhomov, Alex, Al Sicignano & Tim Goldburt. 2004. "Lab Testing of New Seismic Sensor for Defense and Security Applications." *Proc. SPIE 5611, Unmanned/Unattended Sensors and Sensor Networks*. https://doi.org/10.1117/12.581376

Palik, Júlia. 2021. "Watchdogs of Pause: The Challenges of Ceasefire Monitoring in Yemen." *International Peacekeeping*, 28:3, 444-469. DOI: 10.1080/13533312.2021.1918004

Pauwels, Eleonore. 2021. *Peacekeeping in an era of converging technological and security threats*. UN DPO Paper. As of 22 March 2022: https://peacekeeping.un.org/sites/default/files/06_24_final_pauwels_converging_ai_cyberthreats_digital_peacekeeping_strategy_1.pdf

Pinaud, Margaux. 2020. "Home-Grown Peace: Civil Society Roles in Ceasefire Monitoring." *International Peacekeeping*, 28 (3): 470-495. As of 13 April 2022: https://doi.org/10.1080/13533312.2020.1861943

Principles for Digital Development. N.d. "Context Analysis of Technologies in Social Change Projects." As of 22 March 2022: https://digitalprinciples.org/wp-content/uploads/Context-Analysis_Framework_v3-1.pdf

Puttick, Miriam. 2017. *Eyes on the Ground: Realizing the potential of civilian-led monitoring in armed conflict*. Ceasefire Centre for Civilian Rights and Minority Rights Group International. As of 18 March 2022: https://www.ceasefire.org/wp-content/uploads/2017/08/EYES-ON-THE-GROUND-Realizing-the-potential-of-civilian-led-monitoring-Ceasefire-July-2017.pdf

Rudnick, Lisa, Joseph Guay & Leeor Levy. 2020. *Myanmar Civilian Monitoring Initiative Learning Phase Final Report: Navigating Opportunity & Risk in the Digital Age*. Elrha. As of 22 March 2022: https://www.elrha.org/wp-content/uploads/2020/03/HIF_Myanmar-PR_Final-Draft.pdf

Schneibel, Anne. 2021. "Using satellites as independent observers." Techpops, 1 September. As of 16 March 2022: https://tech-blog.zif-berlin.org/using-satellites-independent-observers

Security Council. 2016. "Report of the Secretary-General on the situation in Mali." S/2016/281. As of 16 March 2022: https://minusma.unmissions.org/sites/default/files/160328_sg_report_mali_english.pdf

Tanner, Fred. 2021. "The OSCE and Peacekeeping: Track Record and Outlook." In IFSH (ed.), *OSCE Insights* 4/2021, Baden-Baden: Nomos, 2022. As of 18 March 2022: https://doi.org/10.5771/9783748911456-04

United Nations Peacekeeping. 2020. *Strategy for the Digital Transformation of UN Peacekeeping*. As of 16 March 2022: https://peacekeeping.un.org/sites/default/files/20210917_strategy-for-the-digital-transformation-of-un-peacekeeping_en_final-02_17-09-2021.pdf

United Nations. 2021. "Secretary-General Outlines Elements of Digital Transformation Strategy for Peacekeeping, at High-Level Security Council Debate." United Nations Meetings Coverage and Press Releases, 16 August. As of 22 March 2022: https://www.un.org/press/en/2021/sgsm20856.doc.htm

The UN Refugee Agency (UNHCR). 2015. "Biometric Identity Management System." As of 13 April 2022: https://www.unhcr.org/protection/basic/550c304c9/biometric-identity-management-system.html

Ushahidi. N.d. "The Ushahidi Platform." As of 18 March 2022: https://www.ushahidi.com/features

Verjee, Aly. 2019. *Monitoring ceasefires is getting harder: greater innovation is required*. Oslo Forum Peacewriter Prize 2019. As of 22 March 2022: https://www.hdcentre.org/wp-content/uploads/2019/07/Oslo-Forum-Peacewriter-Prize-2019.pdf

Whiteflag. N.d. "Frequently Asked Questions." Whiteflag Protocol. As of 22 March 2022: https://www.whiteflagprotocol.org/faq/

Wittkowsky, Andreas. 2021. "Human or Machine? Lessons from the Use of Technology in the Monitoring Mission to Ukraine." The Global Observatory, 12 April. As of 22 March 2022: https://theglobalobservatory.org/2021/04/lessons-from-use-of-technology-in-monitoring-mission-ukraine/

EXPLORING THE USE OF TECHNOLOGY FOR REMOTE CEASEFIRE MONITORING AND VERIFICATION

Ceasefires play an important role in the prevention of further conflict and armed violence. Monitoring and verifying that the terms of a ceasefire agreement are respected plays a key role in ensuring an end to violence.

Traditionally, ceasefire monitoring and verification has been human-led. In some circumstances, it can however be difficult deploy observers on the ground. While technology cannot replace humans in all aspects of the monitoring and verification of ceasefires, especially within dialogue and de-escalation efforts, technology can nonetheless support and complement human-led activities.

This report explains what technological solutions are available to help monitor and verify ceasefires, outlining the respective technological advantages and limitations of each solution. The report also provides a series of guiding considerations around the use of technology, highlighting recommended issues to reflect upon before using technology to aid with ceasefire monitoring and verification.

UNIDIR