BRILL
NIJHOFF

SECURITY AND HUMAN RIGHTS (2020) 1-12

SECURITY AND
HUMAN RIGHTS
brill.com/shrs

Analysis for Peace: *The Evolving Data Tools of UN and OSCE Field Operations*

A. Walter Dorn
Professor of Defence Studies, Royal Military College and Canadian Forces College, Toronto, Canada
walter.dorn@rmc.ca

Cono Giardullo
Associate Fellow, Istituto Affari Internazionali, Rome, Italy
conogiardullo@gmail.com

Abstract

Both the United Nations and the OSCE are working to improve their peace operations technologically. While the emphasis is more often placed on new collection tools (e.g., satellite imagery, UAVs, night-vision tools, etc.), the challenge remains to exploit the imagery and the copious other data that has been collected. By examining the software and evolving methods used by UN operations and the OSCE Special Monitoring Mission in Ukraine, we evaluate two often neglected steps of the information/intelligence cycle: analysis and dissemination. Lessons are drawn from both UN and OSCE experience in war-torn locations. Both organizations still need to establish strong and effective data-analysis and -sharing systems within their missions, and to find better ways to share information with the conflicting parties, and with humanitarian partners.

Keywords

dissemination – intelligence – OSCE – peacekeeping – Special Monitoring Mission – technology – United Nations – UAV

Introduction*

Peace operations have frequently provided dramatic evidence of violations of peace agreements. Increasingly, these revelations are made possible by advanced technologies. For example, the OSCE Special Monitoring Mission to Ukraine (SMM) used unmanned aerial vehicles (UAVs) to identify breaches of the Minsk agreements on both sides of the line of contact. For example, the mission's long-range UAVs detected Russian trucks entering the non-government (rebel) held territory at night through dirt roads, far from the border points with the Russian Federation that the OSCE regularly monitors.[1] Other SMM UAV imagery has shown the unauthorized presence of specialized military vehicles, including sophisticated jammers.[2] Imagery also showed military vehicles from both sides hiding under the cover of half-destroyed houses or positioned in or near schools and kindergartens. The SMM also produced 3D renderings of extensively damaged civilian housing on both sides.[3]

The SMM also went public with recorded attacks on its own monitoring technology, e.g., videos showing surface-to-air missiles and rounds fired in the direction of its UAVs, including rounds from a heavy machine gun.[4] Instances of shooting at UAVs, both on government and non-government controlled sides, were publicized.[5] UAVs were even shot down, causing the SMM to halt flights for several months at a time. In addition, a SMM camera was temporarily blinded while being targeted by bright beams of light.[6] Because of the nature of these

* Funding from the Canadian Pugwash Group to hire a research associate is gratefully acknowledged. The views expressed in this paper do not necessarily reflect the views of the Canadian government or the Department of National Defence.

1 OSCE SMM, *OSCE SMM Spotted Convoys of Trucks Entering and Exiting Ukraine in Donetsk Region*, UAV Video Footage, 2018, https://youtu.be/Ani2YWDLXl0.

2 Dylan Malyasov, "OSCE Release Image of Modern Russian Jamming Systems in Eastern Ukraine," *Defence Blog*, April 3, 2019, https://defence-blog.com/army/osce-release-image-of-modern-russian-jamming-systems-in-eastern-ukraine.html.

3 OSCE SMM, *Damage to Civilian Housing in Eastern Ukraine*, UAV Video Footage, 2019, https://youtu.be/8G9Q_M8mwYw.

4 OSCE SMM, *OSCE SMM UAV Targeted near Betmanove*, UAV Video Footage, 2018, https://www.youtube.com/watch?v=sirVhEQ9b8c; OSCE SMM, *SMM Long-Range UAV Comes under Fire*, UAV Video Footage, 2019, https://youtu.be/T-0HNhIu_Gs.

5 OSCE SMM, "Sides Shooting at #OSCE SMM UAVs – UAF Shooting near Stanytsia Luhanska on 17 May [2016]," Twitter, June 24, 2016, https://twitter.com/OSCE_SMM/status/746330925848494080; OSCE SMM, "#OSCE's Hug: For the 6th Week in a Row, SMM UAV Was Targeted by Small-Arms Fire; on 10 March, near Non-Govt-Ctrl Ternove, Armed Men Fired on UAV, Preventing Technical Monitoring and Endangering SMM UAV Operators. #supportSMM," Twitter, March 4, 2018, https://twitter.com/OSCE_SMM/status/974615462842650624.

6 OSCE SMM, *OSCE SMM Camera at Stanytsia Luhanska Blinded by "LPR,"* UAV Video Footage, 2017, https://youtu.be/jKFDEKgfm10.

monitoring technologies, SMM imagery typically accompanies the public disclosures, making it more difficult for the implicated parties to issue outright denials.

Similarly, the United Nations has used UAVs to document attacks on civilian homes and villages, the movement of mobs and rebel groups, the planting of Improvised Explosive Devices (IEDs), and many violations of ceasefire agreements. In addition, the UN's eyes-in-the-sky also helped its mission in the eastern Congo undertake robust peace enforcement actions (i.e., combat) against illegal armed groups, like the M23 that had attacked villages and cities for years.[7] High power cameras on UAVs and helicopters helped identify M23 positions before the group was neutralized in 2013.

Monitoring technologies have proven useful to both the SMM and UN peace operations because they can increase the observation area and period, especially at night. They can also increase the safety of human monitors, who might not be able to view conflicts in dangerous times or areas. Often monitors are not permitted access to areas of ongoing combat. And when diseases like COVID-19 strike, the monitors have to limit their movements and contacts. So technology takes on added importance.

Much of the attention on these technologies has gone to the hardware employed by these international organizations but little study has been made about the software and methods used to analyse the enormous amounts of information (terabytes) generated by the sophisticated technological devices. Identifying a violation may be a challenge within the thousands of square kilometres of aerial patrols and the many hours of video recordings from ground cameras. What technologies supplement the collection methods?

We examine here the software and methods used by the OSCE SMM and the UN for data analysis and dissemination in their peace operations. By comparing their use of technologies, we can take stock of an important but slow technological improvement in peace operations. A previous article[8] has reviewed and compared the hardware used by the two organizations to gather data. Here, we focus on the two often neglected steps that come after data acquisition in the intelligence cycle: analysis and dissemination. As technologies take on added importance during and after the COVID-19 crisis, the full peacekeeping-intelligence process needs review and improvement.

7 A. Walter Dorn., "Combat Air Power in the Congo, 2004," in *Air Power in UN Operations: Wings for Peace*, ed. A. Walter Dorn (Farnham, UK: Ashgate, 2014), 241–53, https://doi.org/10.4324/9781315566313.

8 Walter Dorn and Cono Giardullo, "Technology Investments Paying Off in Peace operations", *Security and Human Rights Monitor*, June 8, 2020, https://www.shrmonitor.org/technology-investments-paying-off-in-peace-operations/.

Data Analysis

When UAVs were first employed by the United Nations in 2013 as a mission asset in D.R. Congo, there was little software and storage means to go along with them. For instance, full motion video (FMV) from UAVs was stored on hard drives that quickly filled, were unplugged, and stacked up for potential future retrieval. Even today, the United Nations does not have software to go through its past UAV footage to identify all images taken of a specific location. Instead, the UN employs a laborious process to look through flight logs to determine the time a UAV had passed near a given location and then go through the FMV archives, if accessible, to see imagery from that time.

There is a growing gap between the enormous quantities of imagery acquired from UAVs and other camera feeds (all part of UN Big Data generation) and the rudimentary ability for the world organization to analyze the imagery. More complex analysis, employing cutting-edge software for pattern recognition, change/anomaly detection, and a host of other analyses is still needed. Artificial intelligence (AI) could also help considerably with such tasks, especially since actionable intelligence remains a key deficiency for UN missions.

To overcome the same problem in eastern Ukraine, SMM staff have requested specialized AI and machine learning training on offer from certain OSCE Participating States. Open Source Intelligence (OSINT) and remote sensing training began in 2019 and a limited number of Open Source officers work since at least 2017 at the mission's headquarters.[9]

The mission in Ukraine faces similar issues as UN missions. The data storage capacity of SMM field offices is limited. This obliges UAV technical monitors, i.e., those piloting UAVs and the payload operators, to locally store the feeds from recent months, while the rest is kept only at a headquarters level. Over time, more and more of sensor streams were fed to headquarters in real time and centralized there. Despite that, most monitors have relatively easy access to recent data. When operational necessity arises, field staff can ask to retrieve flight logs and images to identify particular challenges in their areas of responsibility.

SMM reporting officers who compile information for mission reports also encourage patrols to attach UAV imagery as well as their handheld camera pictures to their patrol reports, especially to complement the most controversial field assessments, i.e., the direction of fire in impact site assessments, conducted in kinetic areas, where monitors cannot stop for too long without putting themselves in unacceptable danger or being ordered to move out of a

9 OSCE SMM, *Open Source Officer*, 2017, https://jobs.osce.org/vacancies/open-source-officer-vnsmus00621.

kinetic area by security officers. Monitors are bound by the code of conduct and by an additional internal pledge not to share the images outside of the mission.

Both the UN and the SMM are able to request commercial satellite imagery and evaluate UAV/satellite imagery in order to orient operational plans, though still not for real-time support. In particular, these images and videos are used for in-house training and briefings. When imagery can be acquired in near-real-time, the peacekeepers can take better informed actions on the ground.

Unlike UN peacekeeping, which has a Force Generation Service, the SMM relies on *ad hoc* contributions from the OSCE Member States. Based on national geo-political agendas and resources, national support varies greatly. Some countries fund software like the SMM's Enterprise Geographic Information System (EGIS), which is billed as "state-of-the-art reporting and mapping tools [...] to improve the flow of information between the SMM's field teams and its headquarters."[10] Other countries provide essential technological hardware, such as thermal cameras, and, during the COVID crisis, hand sanitizers for monitoring officers.[11]

In UN operations, Member States contribute contingents that often bring their own equipment and analytical tools with them. Units from the global North typically bring advanced hardware and software. For instance, Germany contributed a long-endurance UAV system, the satellite-guided Heron UAVs with pilots and payload managers, to the UN mission in Mali. In addition, the FMV was transmitted to Germany in real-time so that a team of analysts could review the footage. This kind of "back-office" provided the UN with a mission analysis within 48 hours after each flight. But information processed by technologically advanced countries is not always shared with the UN mission. Such was the case in the UN mission in Mali when The Netherlands helped set up the All Sources Information Fusion Unit (ASIFU) and offered the "TITAAN" database system.[12] The information system provided security at a NATO-standard, but

10 Stefano Toscano, "Interviews with HMA Directors: Ambassador Stefano Toscano," *The Journal of Conventional Weapons Destruction* 23, no. 1 (May 2019): 9, https://commons.lib.jmu.edu/cisr-journal/vol23/iss1/4.

11 OSCE SMM, "OSCE SMM Status Report as of 23 March 2017," Status Reports of the Special Monitoring Mission to Ukraine (Kyiv, Ukraine: OSCE, March 3, 2017), https://www.osce.org/files/f/documents/e/c/306911.pdf; Government of Canada, "Delighted to Work w @LT_OSCE to Provide Hand Sanitizer to the @OSCE_SMM for Use by Its Monitors Working in Ukraine. The Safe Realisation of the SMM's Full Mandate Is a Responsibility We All Need to Support.," Twitter, April 28, 2020, https://twitter.com/Canada2OSCE/status/1255183692626104321.

12 Sebastiaan Rietjens and A. Walter Dorn, "The Evolution of Peacekeeping Intelligence: The UN's Laboratory in Mali," in *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law*, ed. Floribert Baudet et al. (The Hague: Asser Press, 2017), 197–219, https://doi.org/10.1007/978-94-6265-183-8_9.

with NATO-clearances required to access the data, so much of the information never reached the rest of the UN mission, except for selected persons from NATO countries. Other parts of the mission used a much simpler system call SAGE, sometimes spelled out in UN documents as Situation Awareness Geospatial Enterprise, which is based on the Ushahidi open-source software. It serves as a repository of information on events and incidents. An upgraded platform called UniteAware, based on software from the company ESRI, expands on SAGE by adding tracking and patrol planning elements. It has been successfully pilot-tested in the UN mission in the Central African Republic (MINUSCA) and is now being rolled out to other peacekeeping missions as a standard mission tool. The UniteAware features and capabilities are slowly growing.

Both these systems (the SMM's EGIS and the UN's UniteAware) aim at developing predictive peacekeeping to identify threats as early as possible in order to kick start early action.[13] In addition, tracking peacekeepers is possible using UN mission radios (handheld and vehicular) and potentially cell phones through UniteAware, so UN missions are in a better position to move the right peacekeepers to the right location in a comparatively short time in order to prevent or mitigate an identified threat.[14]

Attribution and More

The UN and OSCE missions possess the technical and analytical capabilities to attribute responsibility for most of the violations they observe. However, both organizations experience political constraints, with some missions like the SMM burdened with mandates that limit the inquiry and attribution actions at their disposal. The United Nations is not restricted by its mandate to publicly identify the perpetrators of violations but it does fear blowback from vengeful violators who might attack the UN or the local population or try to discredit the good name of the UN. Still, the UN is rarely bound by its mandate from naming perpetrators. This is one of the marked differences between the SMM and the UN peace operations.

The SMM's strict mandate does not allow it to attribute ceasefire violations to the violator, even when the identity of the guilty party is well established

13 Allard Duursma and John Karlsrud, "Predictive Peacekeeping: Strengthening Predictive Analysis in UN Peace Operations," *Stability: International Journal of Security and Development* 8, no. 1 (February 2019): 1–19, https://doi.org/10.5334/sta.663.

14 A. Walter Dorn and Christoph Semken, "Blue Mission Tracking: Real-Time Location of UN Peacekeepers," *International Peacekeeping* 22, no. 5 (October 2015): 545–64, https://doi.org/10.1080/13533312.2015.1094192.

(e.g., Ukrainian government, Russian or separatist forces or others). Ironically the SMM usually publicly presents the precise evidence of such violations, more so than the UN. So even the casual observer from the public could easily infer who committed the violations. Furthermore, the SMM cross-checks its information carefully from the visual/audible accounts of monitors (e.g., of gunshots) and the mission's technological means, summarized in technical quarterly reports:[15] UAVs, cameras, acoustic sensors, and satellite images. But in the end, the SMM cannot publicly identify violations of ceasefire, though other types of violations are not subject to this restriction.

UN operations can attribute the source of violations but remain quite shy about naming and shaming perpetrators because the mission has to deal with the same parties at the negotiating table, where it often plays the role of an impartial mediator – a responsibility that is partly also on SMM's shoulders, given its role in the Minsk negotiation talks.

Ironically, while not attributing the source of violations, the SMM is extremely transparent and goes public daily with its observations. The UN reports violations far less frequently, focusing rather on extensive thematic and more general reports, including reports to the UN Security Council every three to six months.

Data Dissemination

To be useful for a mission, analysed information – sometimes called peacekeeping-intelligence by the UN – needs to be provided not only to top decision-makers but also selectively disseminated within the mission and to external partners, including the UN country team (agencies and programmes like UNICEF and UNDP, etc.). Often the benefit is greater when it is disseminated publicly as well, if sensitivity allows. Both the SMM and the United Nations lack a "secret" level of classification because they have not established the means for information handling at that level. The highest classification level in the UN is "Strictly Confidential," which applies to information "whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to, or impede the conduct of, the work of the United Nations."[16]

15 See for example: OSCE SMM, "January – March 2020 Trends and Observations from the Special Monitoring Mission to Ukraine," Trends and observations from the Special Monitoring Mission to Ukraine (Kyiv, Ukraine: OSCE, April 15, 2020), https://www.osce.org/files/f/documents/0/d/450175.pdf.

16 United Nations Secretary-General, "Information Sensitivity, Classification and Handling," Secretary-General's Bulletin (New York, NY: United Nations, February 12, 2007), para. 2.3, United Nations Dag Hammarskjöld Library, https://undocs.org/en/ST/SGB/2007/6.

The SMM only adopts the label "OSCE – for internal use only", often used for remote sensing classified images, and "OSCE Restricted" for the highest classification. The daily operational tasking plan also has this classification on it, requesting monitors to safely use and recycle/destroy the document.[17]

After the TITAAN system was withdrawn from Mali in 2016, the UN established the "Mali Mission Secure Network" (MMSN) to convey information more securely among specific elements of the mission. This costly system is administered by a French contractor, and is the most secure system that the UN has yet employed in the field.[18] The UN should be able to learn from the contractor how to improve the security of the UN's systems, so it can gradually replicate and replace many of the desired security features.

Though the UN still uses the term "code cable" for high-level communications from the field, the field missions communicate situation reports to UN headquarters by secure email on a daily and weekly basis, with flash reports sent for more urgent matters. And mission heads speak periodically (e.g., semi-annually) before the Security Council. But, as mentioned, UN missions rarely provide daily reports of ceasefire violations to the public, unlike the SMM.[19]

In the SMM, the exchange of information is well established with so-called "mandated partners" i.e., the OSCE executive structures, the United Nations—especially the Resident Coordinator, UNHCR, OHCHR, and OCHA—and the Council of Europe.[20] Like mandated partners, the International Committee of the Red Cross (ICRC) also receives large amounts of information from the SMM. But there is no internally agreed system—a "shareability matrix"—to guide how data derived from remote sensing and cameras are shared. The rule of thumb is that raw imagery can only be used inside the Mission, while derived (or annotated) products can be shared with mandated partners and/or the general public upon the approval of Chief Monitor, one of the deputies, or exceptionally of Head of Unit (i.e., Reporting, Operations, Press and Public Information, Human Dimension). Approval is more easily given to distribute analyses among mandated partners than through publication on social media or official reports.[21]

17 Based on personal experience of one of the authors who served in the SMM.

18 Rietjens and Dorn, 2017.

19 A. Walter Dorn, *Keeping Watch: Monitoring, Technology & Innovation in UN Peace Operations*, UN University Press, 2011.

20 Permanent Council of the OSCE, "Deployment of an OSCE Special Monitoring Mission to Ukraine," OSCE Permanent Council Decision (Vienna, Austria: OSCE, March 21, 2014), para. 3.7, https://www.osce.org/files/f/documents/d/6/116747.pdf. The UN acronyms are: UNHCR for United Nations High Commissioner for Refugees; OHCHR for Office of the High Commissioner for Human Rights; and OCHA for Office for the Coordination of Humanitarian Affairs.

21 Based on personal experience of one of the authors who served in the SMM.

Both UN and SMM missions use dedicated websites and social media accounts to share announcements and views with the general public.[22] In the SMM, Twitter is used primarily for daily reports and specific products, such as "trends and observations" quarterly reports and status reports, as well as a general overview of the SMM's main activities.[23] For instance, the daily and "Spot" reports from the SMM are available on the OSCE website.[24] The UN usually does not publish its daily reports. But some force commanders, such as Lieutenant General Dennis Gyllensporre of the UN peacekeeping mission in Mali, are avid tweeters who provide frequent (e.g., daily) updates on recent mission activities, including combat operations. The caveat that comes with the Twitter feed from @Gyllensporre is important: "[o]pinions expressed are my own."

Information dissemination outside the SMM is useful in at least two ways. First, it helps negotiations. Chief Monitors of the SMM have been invited several times to brief the UN Security Council via video conference, and they present their quarterly reports to the OSCE Permanent Council in person.[25] Other meetings, like the regular Embassy meetings in Kyiv, or informal Human Dimension briefings,[26] offer the opportunity to brief the OSCE Member States with drone pictures and videos.[27] Such sharing helps to establish a level playing field among the Participating States so that discussions are well informed when decisions are taken. Remote sensing imagery has also been used in Minsk during the bimonthly negotiation talks, for example, contributing to the successful negotiations to restoring the broken Stanytsia Luhanska bridge.[28] Second, the SMM has established a system of humanitarian referrals in the

22 The UN missions have websites at unmissions.org, for instance minusma.unmissions.org is the URL for the Mali mission. The SMM website is https://www.osce.org/special-monitoring-mission-to-ukraine and SMM reports and updates can also be found at https://www.osce.org/ukrainecrisis.

23 OSCE SMM, https://twitter.com/osce_smm?lang=en.

24 OSCE SMM, "Daily and spot reports from the Special Monitoring Mission to Ukraine," updated daily or even more frequently, https://www.osce.org/ukraine-smm/reports.

25 "Briefing on the Political Situation in Ukraine," *What's In Blue*, April 27, 2016, https://www.whatsinblue.org/2016/04/briefing-on-the-political-situation-in-ukraine.php.

26 OSCE Member States' organized human dimension meetings at OSCE HQ in Vienna focus either on a broad specific human rights topic or on the main violations of human rights recorded within a field mission area. Based on personal experience of one of the authors who served in the SMM.

27 OSCE SMM, "Today, in Vienna the @OSCE SMM Held an Informal Human Dimension Briefing to the #OSCE Participating States Which Focused on Civilian Hardship in #conflict-Affected Areas in Eastern #Ukraine," Twitter, July 18, 2018, https://twitter.com/OSCE_SMM/status/1019646750863314945.

28 OSCE SMM, "Image of 'Broken Section of Stanytsia Luhanska Bridge' Taken via Mini UAV on 18 September 2019," Facebook, November 22, 2019,

field to inform partners and trusted NGOs about urgent humanitarian needs.[29] Findings obtained through advanced surveillance technology are often shared, but this does not include SMM images and videos, at least not often.

In each mission, a balance must be found between the need for open and frequent sharing of information, including with the conflicting parties for confidence-building, and the need to prevent the misuse of the information by the conflicting parties or others for one-sided advantage. Also, peace missions must sometimes refrain from sharing information to avoid revealing the sources and methods of information gathering, though this is much less of a factor than in national intelligence systems.

Conclusions

The SMM, throughout its relatively short history, has proven comparatively speedy and highly ductile in deploying advanced technologies, even as the regional political landscape changed, and as the conflicting parties struggled to gain advantage. The trust provided to the SMM was exemplified when in 2019 the OSCE Participating States expanded the mission mandate to monitoring over new and large areas, including observing any restrictions to the freedom of navigation in the Sea of Azov and the Kerch Strait.[30] Also, in December 2019, Normandy Four Leaders (leaders of Germany, Russia, Ukraine, and France) asked[31] the mission to expand SMM monitoring to 24/7, a measure that, because of the outbreak of COVID-19, has not yet been operationalized. This resulted in an 8 per cent increase in the budget needed to implement the tasks, which include an increase in surveillance capacity.[32]

---

https://www.facebook.com/oscesmm/photos/pcb.1438325879652446/1438325732985794; OSCE SMM, "Image of 'Repaired Section of Stanytsia Luhanska Bridge' Taken via Mini UAV on 21 November 2019," Facebook, November 22, 2019, https://www.facebook.com/oscesmm/photos/pcb.1438325879652446/1438325769652457/.

29 Ertugrul Apakan and Wolfgang Sporrer, "Comprehensive Security in a Conflict Environment," *Security and Human Rights* 29, no. 1–4 (December 2018): 83–89, https://doi.org/10.1163/18750230-02901001.

30 Permanent Council of the OSCE, "Extension of The Mandate of the OSCE Special Monitoring Mission to Ukraine," OSCE Permanent Council Decision (Vienna, Austria: OSCE, March 29, 2019), https://www.osce.org/files/f/documents/4/a/415988.pdf.

31 Stephanie Liechtenstein, "Normandy Summit Discusses Expanding Mandate of OSCE SMM," *Security and Human Rights Monitor*, December 19, 2019, https://www.shrmonitor.org/normandy-summit-discusses-expanding-mandate-of-osce-monitors-in-ukraine/.

32 Stephanie Liechtenstein, "Diplomacy in Times of Lockdown," *Security and Human Rights Monitor*, March 24, 2020, https://www.shrmonitor.org/diplomacy-in-times-of-lockdown/.

The UN record in technological innovation is more mixed. Some missions have expanded the use of monitoring technologies, while others have hardly deployed them. Ironically, one of the UN's oldest missions, the peacekeeping force in Cyprus, was the first to deploy (since 2005) remote cameras in hotspots to monitor activities and violations. The more recent missions in Mali and the Central African Republic deployed aerostats for certain periods and contracted new UAV and fixed-wing (manned) surveillance platforms. The Central African mission also expanded its analytical capacity by testing and adopting the UniteAware software. The Mali mission is exploring public radio monitoring using automated transcription and translation from local languages. Overall, the UN's capacity for data analysis and dissemination is slowly increasing.

The UN and the OSCE are both wrestling with improving data analysis and dissemination in their field missions. Lessons can be drawn by comparing the two organizations. The OSCE's SMM is moving ahead with EGIS. The mission also offers daily reports on ceasefire violations, which the UN rarely does. The SMM is still reluctant to share relevant humanitarian data with partners. Since sharing rules are sometimes hard to interpret,[33] the mission limits cooperation, which does not help promote success stories from humanitarian responders that could benefit the SMM's reputation in the country. The UN, as a complex organization with multiple agencies and programmes present in the field, has been quicker and more proactive from this point of view, analyzing and sharing information with the UN country team, especially through the Office for the Coordination of Humanitarian Affairs (OCHA). In addition, the UN Secretary-General has put forward a "Data Strategy" for the organization, with one of the goals being "a culture that values openness & sharing by default."[34] The UN has embraced cloud computing, so most of the field mission data resides at the Global Services Centre (Brindisi and Valencia) and on contracted cloud services (mostly from Microsoft).

The UN could learn from the SMM about expanding the development of internal field capacities, as opposed to contracted or outside services. Despite the high level and quick deployment speed of the technology, the SMM favored training its monitors, especially to pilot short and mid-range UAVs, and in

33 Ertugrul Apakan and Cono Giardullo, "UAVs for the benefit of people: The use of Unmanned Aerial Vehicles Within the OSCE Special Monitoring Mission", *Human Rights Quarterly*, vol. 42, no.2, May 2020, 486.

34 UN Secretary-General, "Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity 2020–22," https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf), OCHA's already open approach is exemplified by the Humanitarian Data Exchange, https://data.humdata.org.

imagery analysis, instead of hiring outside contractors. However, the larger UAVs in both the UN and the SMM are piloted by contractors, with one country (Germany in the Mali mission) also flying long-range (satellite-guided) UAVs.

Both the UN and the OSCE are far behind many national capacities for data analysis and secure sharing. Their means are far from the cutting edge of software used by advanced military and civilian agencies. And the benefits of artificial intelligence and machine learning are still to be explored in these missions. But the organizations are moving forward in their technological and analytical capability, as they perform their important work to help develop peace in war-torn parts of the world.