Thematic Research Paper for the DPO Peacekeeping Technology Strategy

Enhancing the use of digital technology for integrated situational awareness and peacekeeping-intelligence

Dirk Druet
Center for International Peace and Security Studies, McGill University
April 2021

CONTENTS

1. INTRODUCTION[1]

a. What's changed, what hasn't, and why does it matter?

1. The use of digital technologies for monitoring, surveillance, analysis and decision making in UN peacekeeping operations is **not new**. UN infantry battalions have always possessed a military intelligence arm as one of their twelve core functions.[2] The Brahimi report of 2000 argued that "for complex operations, [missions] should be afforded the field intelligence and other capabilities needed to mount an effective defence against violent challengers,"[3] a position echoed more recently and emphatically in the 2017 "Cruz report."[4] And analysts have identified a wide array of digital technologies that have been deployed in missions over the years to enable and enhance their ability to monitor and analyze their surroundings.[5]

2. What ***is* new** are the types of threats and trends that missions seek to understand; the power and sophistication of the capabilities available to peacekeeping; the volume and structure of data they generate; and the complexity of the management of these tools in a peacekeeping environment. Let us address these trends in turn.

3. Across many operations, peacekeepers are being asked to interact more proactively with **increasingly dynamic threats**. Expectations around the protection of civilians are higher than ever and, combined with budgetary and political pressures to downsize missions, they have prompted several missions, notably UNMISS and MONSUCO, to adopt centralized but highly mobile concepts of operations. These concepts foresee real-time situational awareness across enormous geographic areas to enable rapid projections of force to protect civilians. At the same time, peacekeepers in some missions are coming under diverse forms of direct attack from conflict parties and, in some cases, civilian populations, demanding comprehensive and real-time tactical awareness of their immediate surroundings as well as a nuanced understanding of local perceptions, political discourse, and the information environment in which they operate.

4. The capabilities of the digital technologies that are accessible to peacekeeping missions today are **exponentially more powerful** than those of a decade ago. As the 2015 report of the DPKO-DFS Expert Panel on Technology and Innovation pointed out, continually improving camera resolution, the accuracy and availability of aerial and geospatial data, and movement detection sensors have been employed for a broad array of intelligence and situational awareness purposes in missions, from ceasefire monitoring to camp security.[6] The increase in strength of these tools is such that missions are now capable of mass visual and digital

[1] This paper was prepared by Dirk Druet of the McGill University Centre for International Peace and Security Studies for the UN Department of Peace Operations as an input for the preparation of a new strategy for Technology in UN Peacekeeping Operations. The author is grateful to Eduardo Artigas, Guillaume Criloux, Guillaume Darme, and Rajkumar Cheney Krishnan for reviewing previous drafts of the paper. The views expressed in this paper are those of the author alone and do not necessarily reflect the view of the United Nations.

[2] United Nations, "United Nations Infantry Battalion Manual (UNIBAM), Second Edition", New York: UN Department of Peace Operations, January 2020, p. 14.

[3] United Nations, "Report of the Panel on United Nations Peace Operations", in A/55/303-S/2000/8099, New York: UN General Assembly and UN Security Council, 21 August 2000, paragraph 51.

[4] Lt. Gen. (Ret) Carlos Alberto dos Santos Cruz, "Improving Security of United Nations Peacekeepers: We Need to Change the way we are doing Business", New York: Un Department of Peacekeeping operations, 19 December 2017.

[5] For example, see Walter Dorn, *Keeping Watch: Monitoring, Technology and Innovation in UN Peace Operations,* Tokyo: United Nations University, 2011.

[6] United Nations, "Performance Peacekeeping: Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping", New York: UN Department of Peacekeeping Operations and UN Department of Field Support, 22 December 2014.

surveillance in their operating environments, enabling them to conduct "human terrain mapping" and generate "pattern of life" analyses to identify and isolate threats. While many of these tools are available on the market, the most sophisticated of these technologies have tended to be brought by Member States – either through deployed units or by facilitating arrangements with defence contractors – that bring with them skills, procedures and legal and policy frameworks necessary to meaningfully employ the technologies.

5. What once was decentralized and unstructured – yet substantively rich and deep – information gathered by peacekeepers is now increasingly **centralized and organized data**. Quantitative and qualitative tool are being united to present considerable new opportunities for analysis, if the information can be effectively harnessed. More data-driven analysis tools promise to improve the insights and predictive capacity of mission personnel across a broad range of tasks, from the protection of civilians to political strategies to local conflict prevention, but only if the information can be shared in a way that balances the need for broad access with operational security and human rights concerns. And this richer analytical ecosystem has the potential to revolutionize decision-making in missions, but only if the analysis gets to decision-makers in a format and timeframe that enables them to take decisions on its basis.

6. Finally, these trends have introduced **unprecedented complexity** into how peacekeeping operations acquire, deploy and manage digital technologies for peacekeeping-intelligence and situational awareness. More sophisticated technologies are requiring more detailed and technically challenging processes. Solution design, project management, procurement processes and personnel traditionally used to deploy benign information and communications technologies are now engaging with technologies that demand considered and often novel legal frameworks and ethical considerations. As peacekeeping strives to deliver peacekeeping-intelligence and situational awareness appropriate to its mandates and operating environments, the digital technologies it employs for this purpose come with serious political risks and normative consequences that demand careful consideration.

b. Objectives and scope

7. In this context, this paper asks the question: to what extent are the digital technologies deployed in peacekeeping today **appropriate for and delivering on missions' needs** to generate high quality peacekeeping-intelligence and situational awareness? How can current and new technologies contribute more effectively, and what technical, management, policy and operational strategies would be necessary to ensure that these technologies are employed as effectively, efficiently and responsibly as possible? In asking these questions, the primary objective of the paper is not to introduce a series of new ideas or concepts. Rather, in a management, policy and operational environment that is highly complex, decentralized and, often, heavily politicized, this paper attempts to organize what we know about digital technologies for peacekeeping-intelligence and situational awareness and how they are managed in a way that enables a comprehensive, strategic discussion on DPO's approach to these technologies in the future.

8. Based on a detailed review of policy and strategy documents, a series of confidential interviews with DPO, DOS and DMSPC technology providers and users, and a survey of the academic and policy literature, **the paper proceeds along the following structure**. It begins by surveying the state of digital technologies in use for peacekeeping-intelligence and situational awareness, describing in broad terms their purposes, capabilities and operational

contexts, and considering what impact these have had on peacekeeping-intelligence and situational awareness, both individually and collectively. Finally, the paper identifies a number of opportunities, challenges and strategic questions that have emerged for the future of digital technologies and their outputs as part of the intelligence cycle.

9. It should be noted that the paper addresses policy and management issues **specific to peacekeeping-intelligence and situational awareness**. It does not address broader questions of how technology, in general, is managed in peacekeeping.

c. Terminology

10. *Peacekeeping-intelligence (PKI):* The 2019 DPO Policy on Peacekeeping-Intelligence defines the "fundamental purpose" of **PKI** as aiming to "enable missions to take decisions on appropriate actions to enhance situational awareness and the safety and security of UN personnel, and inform activities and operations related to the protection of civilians," including to a) support a common operational picture to support planning and operations; b) provide early warning of threats to enable timely mission action; and c) identify risks and opportunities.[7]

11. *Situational awareness (SA):* The 2019 DPO Policy on Joint Operations Centres (JOCs) defines **situational awareness** as "knowledge, understanding and anticipation of a situation through monitoring and reporting of current events, analysis and predictive assessments.[8]

12. *PKI/SA:* For the purposes of their interactions with digital technologies this paper treats peacekeeping-intelligence and situational awareness (henceforth, **PKI/SA**) as heavily inter-linked for the purposes of their interaction with digital technologies. This does not imply that the concepts are substantively equivalent. In the interest of simplicity, therefore, this paper uses the PKI cycle – consisting of acquisition, collation, analysis, dissemination, and requirements management – as the framework for identifying how different digital technologies contributes to PKI/SA at different stages of the process.

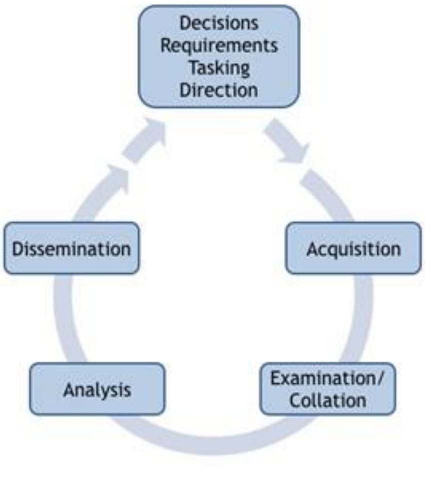

Figure 1. The peacekeeping-intelligence cycle[9]

[7] United Nations, Policy on Peacekeeping-Intelligence, ref. 2019.08, New York: UN Department of Peace Operations, 1 May 2019, paragraph 5.

[8] United Nations, Policy on Joint Operations Centres (JOCs), ref. 2019.20, New York: UN Department of Peace Operations, 1 November 2021, paragraph 48.

[9] United Nations, Policy on Peacekeeping-Intelligence, ref. 2019.08, New York: UN Department of Peace Operations, 1 May 2019, paragraph 5.

2. THE STATE OF PKI/SA DIGITAL TECHNOLOGIES: CAPABILITIES, OUTPUTS AND IMPACTS

13. This section surveys the **principal digital technologies for PKI/SA** in use across peacekeeping operations today, describing their general capabilities and assessing their contributions to the effective and efficient functioning of the peacekeeping-intelligence cycle. This list is not exhaustive; in particular, it excludes relatively small initiatives or mission-specific tool. Rather, it is intended to provide an overview of the strategic positioning of DPO on PKI/SA technologies and identify key areas of added value and challenge. Throughout this section, different types of ***information and analytical outputs*** generated by digital technologies are bolded and italicized.

a. Acquisition: Monitoring, surveillance, and investigation

14. The **acquisition** of information to inform PKI/SA consists of obtaining raw data and information to serve as the basis for analysis. Information is gathered using sensors – technological or human – that identify and record information. Ideally in a PKI cycle, information is acquired on the basis of an "information requirement" that directs the senor to focus on specific targets, questions or areas.[10]

15. Aerial surveillance. While **unarmed, unmanned aerial systems** (UAS) have been used occasionally in peacekeeping operations over the years, the systematic push to deploy them as a standard capability began with the deployment of a UAS in MONUSCO in 2016. Since then, UAS with widely varying ranges and technical sophistication have been used in MINUSCA, MINUSMA and UNMISS, among others. While UAS can carry any number of sensors, those used in peacekeeping missions to date have had been used primarily to produce geotagged still and video photography. UAS have been acquired for missions through three modalities, each with its advantages and challenges. These are covered in turn.

16. *Contingent Owned Equipment:* UAS may be brought into missions as an **organic component of a TCC capability** generated by DPO. This is the case, for example, with the German and Swedish Intelligence, Surveillance and Reconnaissance (ISR) companies deployed to MINUSMA in Gao and Timbuktu, or the French reconnaissance unit in MINUSCA. In this scenario, drones are operated and maintained by the unit and the raw data they generate processed and exploited by the TCC before being turned over to the mission. This usually involves a system of "reach-back" in which data is sent to a centralized facility – usually in the TCC's capital – for processing and exploitation by skilled analysts. Since the UAS are sensitive parts of national intelligence systems, they are invariably subject to stringent operational security parameters, often imposed by national legislation. As such, the initial processing of the data involves the removal of protected categories of data such as sensitive but, for the UN's purposes, unnecessary, telemetry data. In practical terms, this means that military units with COE UAS would generally deliver ***individual, analyzed image or video products***, either on request on or their own initiative, into the PKI/SA cycle.

> Advantages: Since the UAS comes as an organic part of a national ISR capability, the mission benefits, in principle, from **advanced technical expertise** and a variety of related TCC capacities, including exploitation and analysis, potential access to national

[10] Ibid., paragraph 10.3

databases, and information requirement management functions, all of which the UN lacks.

Disadvantages: Since individual products are usually delivered to the mission, data is not available to be stored or queried at a later time by mission personnel from outside the unit. The operational security parameters and national processes around the asset can make **integration into mission processes difficult** and, as discussed below, raises numerous legal, political and ethical questions.

17. *Contracted surveillance services:* UAS may also be operated in a mission as part of a **contracted service package** with a private sector entity, either as a service procured on the market or via a Letter of Assist with a Member State, which in turn acquires the asset and services from a defence contractor. This practice is currently being used to deploy UAS and other surveillance technologies in several missions, including MINUSMA, MONUSCO MINUSCA and UNMISS. In this scenario, drones are operated and maintained by contractors supplied as part of the service package. While the packages generally include some level of data processing and exploitation, the entirety of the system's outputs become the property of the UN and, if the necessary systems are in place, can be stored and queried indefinitely. The outputs of these systems, therefore, include both ***individual, analyzed image or video products and large volumes of unexploited image and video data.***

Advantages: Since contracted systems are not subject to national security laws and policies, they are **more easily integrated** into the mission's PKI/SA processes and structures and comply more closely with UN data ownership, oversight and transparency standards (though this may not be the case for all Letter of Assist arrangements). The UN's ability to maintain custody of the system's raw data creates, in principle, an opportunity for a broader array of uses by a more diverse set of analysts.

Disadvantages: Missions have experienced challenges in holding UAS providers accountable for the **quality of their systems** and outputs. A large share of maintenance and operational requirements generally falls on the mission.

18. *UN Owned Equipment:* In a third scenario, an individual drone could be procured by a mission and **operated and maintained by mission personnel** such as a uniformed unit with existing expertise (i.e., an ISR unit minus the drone) or even civilian personnel. To the author's knowledge, this practice has only been used to date for micro-drones provided to infantry battalions. This model gives rise to several scenarios. If operated by civilian personnel, the UAS would be operated much like any other mission ICT asset. If operated by a uniformed unit, the UAS would be operated much the same as the COE model, but the ***output would be more akin to the service package model.***

Advantages: An organic, UNOE UAS solves many of the legal and political challenges presented by the COE model. It would deliver a **maximum of raw data** to the mission and could over time build the UN's expertise in UAS management.

Disadvantages: The model involved the heaviest maintenance and operational burden on the mission. If the mission lacked the operational and analytical expertise to effectively employ the system and exploit the data, the output could be sub-par.

19. In addition to UAS, aerial surveillance is also conducted in missions using **manned aerial systems**, including aircraft and helicopters equipped with cameras of various kinds in MINUSMA, and visual helicopter reconnaissance sorties performed regularly in MINUSCA and MONUSCO.

20. Criminal forensics*:* The concept of **intelligence-led policing** provides that UNPOL should acquire criminal intelligence, either as part of operational support to host-state police or in the conduct of interim policing, and that this information should be used to prevent crime, pursue or apprehend an offender, and obtain convictions. Tools for gathering such information could include electronic, photographic and related surveillance devices, which must be a) used in accordance with the procedures established by the Head of the Police Component and b) not conflict with the laws of the host state.[11]

21. The most sophisticated digital technologies used to collect criminal intelligence in peacekeeping have been deployed in MINUSMA. These include IED forensic technologies, for which an UNPOL lab in Bamako possess tools ***to exploit IED remnants for identifiable information*** and, in partnership with bilateral and multilateral partners, can contribute this information for comparison with international databases. IED forensics work has also been conducted by military units in the mission generated specifically for this purpose. In addition, anecdotal evidence suggests that, as part of UNPOL's support to national building efforts, the mission has also contributed and/or provided information to authorities from technologies to analyze the contents of mobile phones retrieved from suspects and related technologies.

22. Camp security and static surveillance: As peacekeeping mission bases have regularly come under direct attack in recent years – notably by mortars and VBIEDs in Mali, but also in CAR and DRC – more focus has been placed on **digital technologies for camp security**. The UN's initial foray into this field is largely seen as a failure: early into the MINUSMA mandate, an aerostat contracted from a French private sector supplier was deployed above the mission's compound in Kidal. As one former MINUSMA staff member who worked on the initiative put it, supply chain challenges in supplying helium to make keep the aerostat afloat, its susceptibility to shrapnel from mortar explosions and gunfire, and its complex operating procedures meant that system was inoperative more often than not. Moreover, a lack of procedures and training meant that the link between threat information from the aerostat rarely led to concrete action by peacekeepers tasked with camp perimeter security.[12] A subsequent independent review of camp security arrangements in Mali fielded by the Government of Israel revealed critical failure points, particularly in terms of the interface between digital technologies and mission processes and procedures. [13]

23. Since then, OICT has led an initiative to deploy more comprehensive suites of camp protection technology across multiple peacekeeping operations to deliver ***actionable, tactical information on imminent threats***. The UN has signed contracts with three contracts with companies – two Israeli contractors and a Belgian subsidiary of a third Israeli contractor – that allow it to submit tailored requirements for security technologies and services at a given site and are provided with quotes from three Israeli military contractors from which to choose. One UN technology expert described the arrangement as "you bring the problem, they give

[11] United Nations, "Guidelines on Police Operations in United Nations Peacekeeping Operations and Special Political Missions", ref. 2015.15, New York: UN Department of Peacekeeping Operations and UN Department of Field Support, 1 January 2016, paragraph 46.

[12] Interview, Former DPO personnel, 5 November 2020.

[13] Interview with DOS/DMSPC personnel, 8 February 2021

you the solution."[14] The solution in Kidal, for example, now includes mortar detection equipment, surveillance tools, and a command centre to manage the various tools coherently.

24. Signals intelligence: A signals intelligence unit has been considered for deployment in MONUSCO since the Force Intervention Brigade was mandated with the offensive task of "neutralizing armed groups" in eastern DRC.[15] Planning processes and political concerns caused the deployment to be delayed for several years but, recently, the process of deployed a unit has reportedly moved forward. Journalistic reporting suggests that the digital technologies deployed with the unit consist of ***international mobile subscriber identity (IMSI) catcher*** technology, the first time such a tool has been officially deployed in a peacekeeping operation.[16]

25. Community alert networks and social media: Digital technologies have been employed increasingly systematically over the past decade to collect information to inform analysis of protection of civilians threats. As part of Community Alert Networks, missions have distributed mobile phones to assist communities in advising the mission of ***information on imminent threats at the community level*** but also "enhancing and organizing their means of communication" within the community.[17] Less formally but with increasing regularity, mission personnel monitor threats via WhatsApp groups, providing rapid but difficult-to-verify information on individual and generalized threats and, in some cases, exposing mis- and disinformation.[18]

26. Local perceptions and media monitoring*:* Missions have a decade of experience in combining digital technologies with qualitative methods to understand local perceptions of, for example, national priorities, the mission or the peace process to inform political and protection, communications and conflict prevention strategies.[19] These have often included the use of mobile phone messaging and, more recently, social media to query the perception of local populations.[20] More recently, MINUSMA has imported language-to-text transcription tools developed by the UN Global Pulse Kampala Lab and previously deployed in Somalia. The software will allow missions to transcribe, organize and draw ***insights from large numbers of local radio shows***, a popular means of political expression in areas that lack internet connectivity.[21]

b. Collation: Databases and information management

27. **Collation** consists of organizing, structuring and storing data in a way that allows all pieces of information to be analyzed in relation to one another. Collation technologies are therefore usually databases or other information management tools.[22]

[14] Ibid.

[15] United Nations, S/RES/2098 (2013), New York: UN Security Council, 28 March 2013.

[16] For example, see The Daily Star, "Al Jazeera's report a false, fabricated, malicious attempt to debase Bangladesh Army: ISPR", Dhaka: Star Digital Report, 16 February 2021.

[17] United Nations, "Handbook: The Protection of Civilians in United Nations Peacekeeping", New York: UN Department of Peace Operations, 2020, p. 97.

[18] MINUSCA personnel, DPO focus group, held inline 13 January 201.

[19] United Nations, "Guidelines on Understanding and Integrating Local Perceptions in UN Peacekeeping", New York: UN Department of Peacekeeping Operations and UN Department of Field Support, ref. 2014.08, 1 June 2014

[20] Pamina Firchow and Roger Mac Ginty, "Including Hard-to-Access Populations Using Mobile Phone Surveys and Participatory Indicators", *Sociological Methods and Research*, vol. 49, no. 1, pp. 133-160, 2020.

[21] United Nations, Annual Report 2019, New York: UN Global Pulse, p. 11

[22] United Nations, Policy on Peacekeeping-Intelligence, ref. 2019.08, New York: UN Department of Peace Operations, 1 May 2019, paragraph 10.5.

28. Sage database: The Situational Awareness Geospatial Enterprise (Sage) is now deployed in all peacekeeping missions excepts UNIFIL[23] and MINURSO, as well as several special political missions. The core function of Sage is an incident and event database that aspires to replace the voluminous but unstructured daily, fact-based, mixed qualitative/quantitative incident and activity reporting performed by many entities at mission Headquarters and field levels. Sage offers a ***central repository for incident and event information*** that, once populated, can be sorted according to a wide variety of variables, such as type of incident, gender dimensions, location and time.[24] Built from the open-source software Ushadi and using the proprietary ESRI ArcGIS mapping backbone, Sage is managed in the UNOCC and relies on OICT technical in New York and Valencia.[25]

29. IBM i2 iBase: iBase is a relatively sophisticated database system that is part of the i2 analysis suite used by many national security services. In peacekeeping, it has been principally used by JMACs and the All Sources Information Fusion Unit in Mali. Like Sage, it allows the entry of multifaced pieces of information, though at a greater level of complexity, to create a multivariable, highly searchable database. While this database requires data entry like any other, some iBase users have automatically replicated Sage datasets into i2, which then need to be further enriched.[26] Unlike Sage, iBase is focused on the identification of targets and thus also includes the capacity to record and manage ***information on individuals and entities.*** Also unlike Sage, the proprietary software must be purchased as individual licenses and generally also requires proprietary training and a steep learning curve.

30. Unit- or mandate-specific databases: A variety of individual units in peacekeeping missions maintain separate databases, usually on **thematic subjects**, that are unlikely to be integrated into a centralized system in the near future. Child protection units, for example, are mandated[27] by the Security Council to maintain a database on incidents of the six grave violence against children in armed conflict as part of a formal Monitoring and Reporting Mechanism that is co-managed with UNICEF and links to politically sensitive reporting processes in New York.[28] Joint Human Rights Offices in peacekeeping missions contribute to a centralized OHCHR database that contains information on violations and investigations, including sensitive personally identifiable information. It serves a variety of purposes beyond analysis and situational awareness, including for the implementation of the Human Rights Due Diligence Policy, and is closely guarded, although in some cases data has been anonymized and imported into Sage. UNDSS also feeds a parallel, central Security Incident Reporting System (SIRS) in all countries in which it works.

c. Analysis: Trends and prediction

31. **Analysts** examine information to discern meaning. Tools to enhance and facilitate analysis includes technologies that can quickly identify inter-relationships within large

[23] UNIFIL manages a standalone incident tracker.

[24] PAX, "Applying Data for Peacekeeping: Challenges and Opportunities" Conference Report, 14 November 2018. Retrieved from https://protectionofcivilians.org/wp/wp-content/uploads/2020/02/Data-for-Peacekeeping-Conference-Report-14-November.pdf

[25] Interview, DPO personnel, 28 January 2021.

[26] Ibid.

[27] United Nations, S/RES/1612.

[28] United Nations and UNICEF, "Guidelines on Monitoring and Reporting Mechanism on Grave Violence Against Children in Situations of Armed Conflict", New York: UN Department of Peace Operations, Office of the Special Representative of the Secretary-General for Children and Armed Conflict, and UNICEF, June 2014.

amounts of data, pinpoint trends, identify causality in complex systems, and make predictions.[29]

32. Sage analysis tools: In addition to organizing incident and event data in a way that facilitates analysis (e.g. sorting incidents by location), the introduction of PowerBI to the Sage has enhanced its capacity to facilitate the processing and expression of analysis. In principle, Sage can be used to identify ***trends over time***, including cyclical patterns (e.g. local patterns of herder-farmer violence) that could be used to predict future events. The tool can also be used to identify ***spatial correlations*** between different types of events to help with the process of analyzing causality (e.g. the relationship between armed group presence and prevalence of CRSV).

33. Sage has several limitations as an analysis tool. First is the **quality and consistency of data across space and time**. Using the tool to analyze trends requires a high degree of confidence that the volume and type of information entered into the system are consistent across different analysts, offices and mission components. This requires standardization in the threshold for entering an event into the database, a shared understanding of the types of information that should be sought and recorded as part of the entry, and common usage of categorization taxonomy. While the UNOCC has made efforts to mitigate risks of inconsistency, for example by adding an "approval" layer for all entries usually performed by the JOC, it is as yet unclear that mission datasets are satisfyingly consistent across different users. Similarly, effective trend analysis requires consistency in the content and structure of data over time. Even in the most mature use cases for Sage, there is not yet a high quality, mission-wide dataset covering more than two years, though this will presumably be the case eventually.

34. Sage's exclusive **focus on events** also limits its analytical power. It lacks, for example, the capacity to record information on a subject or individual that may not be tied to a specific event, but rather to a source – types of data that are at the core of the IBM i2 suite. The system similarly lacks the ability to record contextual factors that various technological or human sensors might usefully acquire, like the daily price of gold, the weather, or the findings of a local perceptions survey, in a way that integrates easily with the event data. Although other geocoded datasets can be overlayed with the event data in Sage and of course in Unite Aware, that data would need to be recorded elsewhere, limiting the tool's ability to help analysts contextualize events as a one-stop-shop.

35. Third-party social media analysis tools: An increasingly broad array of social media analysis tools is in use in pockets of DPO/DPPA Headquarters and missions, including Crimson Hexagon, Dataminr and Predata. While some of these platforms claim to serve as useful early warning tools, their usefulness for this purpose in peacekeeping contexts is limited by several factors. First, limited internet penetration in many conflict-affected countries and regions creates critical data blinds spots, although this is changing rapidly. Second, even where internet penetration is high, not all populations use social media in a way conducive to meaningful analysis. Third, few, if any, social media analysis tools can offer predictive insights with sufficient geographic precision in peacekeeping contexts to be tactically actionable. Nevertheless, social media analysis tools can assist in providing important contextual information and identifying ***trends in public sentiment***, especially at the national level.

[29] United Nations, Policy on Peacekeeping-Intelligence, ref. 2019.08, New York: UN Department of Peace Operations, 1 May 2019, paragraph 10.6.

36. IBM i2 Analyst's Notebook. Using the iBase database, i2 Analyst's Notebook is primarily used to create visualizations of connected networks to enable ***social, political or economic network analysis***. It is useful for understanding the structures of groups and the positioning of individuals and is thus of relevance to the profiling roles of JMACs and criminal intelligence. Like, iBase, however, it is costly and requires dedicated training, making it more likely to continue being used by small, specialized groups of analysts for specific purposes rather than as a widespread analysis tool.

d. Dissemination: Decision-making and requirements management

37. **Dissemination** is the process of conveying the conclusions of analysis to mission decision-makers. It involves the production of situational awareness or analytical products, be they technological, documentary, or verbal, that respond to an identified need for information.[30]

38. Unite Aware. The Unite Aware platform aims to gather datasets from throughout the missions and structure them into a common data foundation that can then be used to deliver a wide ***variety of reports and visualizations*** to enable situational awareness and decision-making.

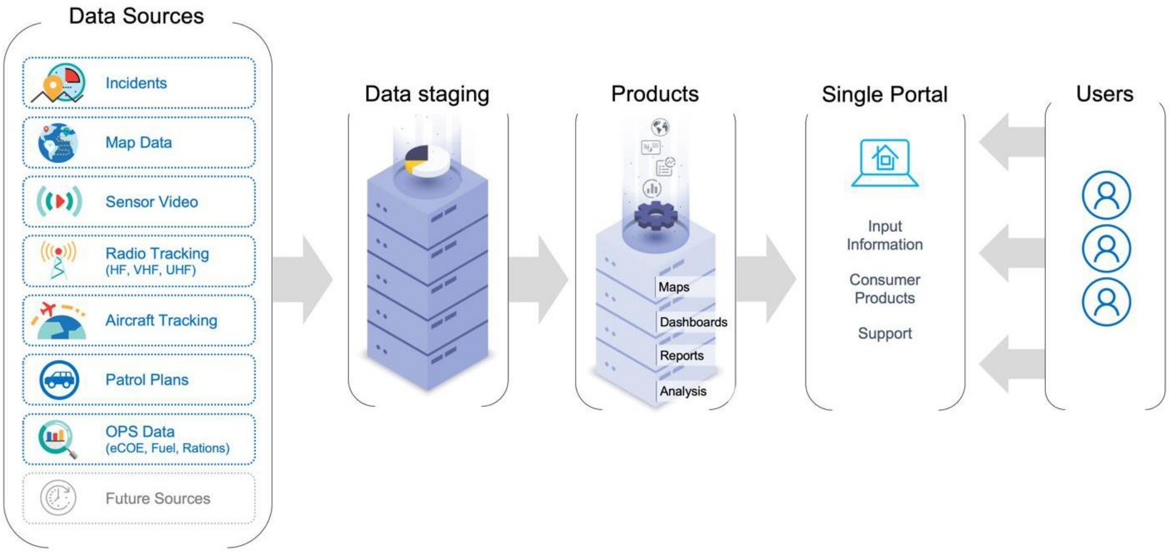

Figure 2. The Unite Aware platform concept[31]

39. As there is currently an ongoing and intensive "Red Team" review of Unite Aware's impact and its prospects for rollout across all of peacekeeping, this paper will not attempt to assess the overall impact of the tool to avoid obfuscating these parallel internal conclusions. However, looking at the platform from a narrow PKI/SA process lens, it is important to note that Unite Aware is currently most tailored to a) **situational awareness dissemination** and b) **peacekeeping-intelligence analysis (but not dissemination)**. The 173 visualization layers developed for MINUSCA consist primarily of location data for different categories of mission

[30] United Nations, Policy on Peacekeeping-Intelligence, ref. 2019.08, New York: UN Department of Peace Operations, 1 May 2019, paragraph 10.5

[31] United Nations, "MINUSCA Pilot: Unite Aware Implementation Project", End of Pilot Report, New York UN DOMSP Office of Information and Communication Technology, October 2019.

assets and processes, such as UN bases and patrol and casualty evacuation routes; and geographic and administrative mapping data, such as local markets and school. For analysis, these datasets and a set of tailored dashboards produced during the MINUSCA pilot are primarily useful as inputs to the analysis process.[32] Analysis products – whether documents, briefings, etc. – would therefore be delivered alongside Unite Aware, using the system to provide visual contexts to the analytical conclusions being presented.

40. As several participants in the Unite Aware "Red team" exercise suggested, for the system to fully serve the intelligence cycle and meet the project's ambitions of becoming a one-stop-shop for situational awareness, it will need to integrate with a **dynamic information requirements management process** that would create a downward flow of information from decision-makers to those gathering, entering and structuring data in the Unite Aware system. This would be most effective and integrative if it included both situational awareness and PKI requirements that could be tasked to sensors and analysts.[33]

41. To "game" this out more tangible, consider the example of a crisis involving an armed group attack on a town. In such a case an initial Unite Aware visualization might overlay Sage incident data with geographic mapping and key civilian structures' location information, giving senior management a clear awareness of the situation. In considering how to respond to the crisis, senior managers might ask both situational awareness questions, such as "where are the current armed forces positions, and how many soldiers are in each unit?", and peacekeeping intelligence questions, such as "what are the likely consequences for the legitimacy of the military if the town were to fall?" In this scenario, and assuming that the DPO Peacekeeping-Intelligence Framework had been implemented in the mission, the **Unite Aware management process would need to integrate closely**, or even be substantively managed by, the mission's Peacekeeping-Intelligence Coordination Mechanism or a similar function in the mission, to ensure an efficient and coherent tasking of the mission's acquisition and analytical assets across all pillars of the mission. The integration of such a process into the Unite Aware platform would represent a significant leap forward in the implementation of PKI cycle management in missions.

42. Social media dissemination: Social media messaging platforms, such as WhatsApp or Signal, are seen as increasingly useful to convey information requiring immediate action. One Head of Office from MONUSCO described WhatsApp as having "revolutionized early warning" by enabling field office/sector-level personnel to **communicate both horizontally and vertically**, delivering messages to company operating bases and providing a 24/7 conduit to national authorities.[34] While the use of WhatsApp is believed by many users to present operational security risks as compared to Signal, the UN's recommended secure messaging platform, the widespread use of WhatsApp by frequently rotating uniformed officers has made it the platform of choice in most missions.[35]

43. Secure networks: Secure networks – i.e. those that ***permit the sharing of information among a sub-set of mission personnel and are resistant to external interference*** – have been cited as a fundamental requirement for a variety of PKI/SA processes, as discussed in further detail below. The requirement for a secure network parallel to standard mission networks was

[32] United Nations, "Annex 3: 173 Visualization Layers Developed for MINUSCA" in "MINUSCA Pilot: Unite Aware Implementation Project", End of Pilot Report, New York UN DOMSP Office of Information and Communication Technology, October 2019.

[33] Interviews, DPO/DPPA personnel, 5 and 9 February 2021.

[34] Interview, MONUSCO personnel, 22 April 2020.

[35] DPO Focus Group, 13 January 2021.

introduced with the deployment of the All Sources Information Fusion Unit (ASIFU) in MINUSMA, which operated on a NATO-standard "Titan Red" system initially supplied by the Netherlands as part of the unit's capacities. When the Netherlands later announced the withdrawal of the system, the UN attempted to design a system to replace it. The result was a system installed and managed by Thales through a Letter of Assist with the French Government.[36] As UN plans to replace the system with one based around a secure Hybrid Cloud and version of Microsoft 365, and as it considers a system to manage signals intelligence data for MONUSCO, it is worth asking deeper questions about the need for and limitations of information security in a UN context (see Section 5).

3. ASSESSING THE COLLECTIVE IMPACT OF PKI/SA TECHNOLOGIES ON ANALYSIS AND ACTION

44. The **collective impact** of PKI/SA digital technologies on the effectiveness of mission operations can be assessed on two levels, first in terms of their impact on the quality of analysis produced by mission PKI/SA entities, and second in terms of how they has influenced mission activities. Neither is easy to do empirically, but anecdotal evidence offers some insight.

45. In terms of **quality of analysis**, there has never been a definitive assessment of the quality of internal peacekeeping analytical products. However, a 2017 analysis of the factual accuracy of UNAMID JMAC reporting over 16 months in 2008-9 could serve as a baseline for one such future analysis. The study compared the events depicted in these reports to those in the widely respected Armed Conflict Location and Event Data Project (ACLED) dataset. While it found that JMAC's reporting was more inclusive of events generally, it was especially more effective at reporting instances of armed conflict that did not involve the Government, which the author attributes to an overreliance on media reporting by ACLED. On the other hand, the study reveals a relatively over-reporting of events that took place in close proximity to peacekeeping bases, suggesting a dependence on the mission's uniformed component for information.[37] This provides a strong basis for a future study to assess whether the mission's reporting one decade hence, after the introduction of Sage and the increased use of digital sensors, has shifted these trends in reporting. Of course, factual accuracy is only one measure of analytical quality; other assessments of mission analytical products before and after the introduction of new PKI/SA tools could, for example, consider the accuracy of predictions, the number of variables used, and the strength and complexity of correlations identified.

[36] Interview, DOS/DMSPC personnel, 8 February 2021.

[37] Allard Duursma, "Counting Deaths While Keeping Peace: An Assessment of the JMAC's Field Information and Analysis Capacity in Darfur", *International Peacekeeping*, vol. 24, no. 5, pp. 823-847, 2017.

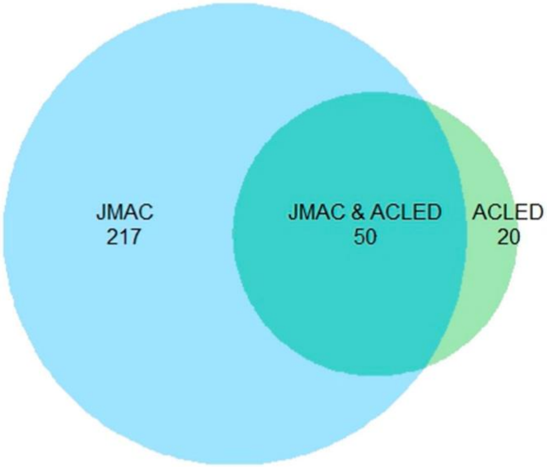

Figure 3. Venn diagram of JMAC vs. ACLED event reporting, UNAMID 2008-9.[38]

46. It is also difficult to measure the **impact on peacekeeping operations** themselves. Given the breadth of PKI/SA products produced by missions, such impacts could presumably range from more astute political strategies to better-targeted programming to more timely tactical responses to security threats. Even in the last, most simple of these three scenarios, as Adam Day, has pointed out, "when confronted with the question of whether a peacekeeping operation has prevented a specific threat to civilians, most of the time the U.N. is unable to answer" because of the methodological challenges in proving the counterfactual, i.e., that, but for the UN's action, an event would have taken place[39]. Moreover, a failure to take effective action in response to a threat does not necessarily reflect on the quality of analysis about that threat.

47. Again, **anecdotal evidence** sheds some light on how peacekeeping missions have or have not benefitted from more technologically driven PKI/SA tools. A former Force Commander once opined that the MINSUMA All Sources Information Fusion Unit's data- and surveillance-intensive, technology-heavy strategic intelligence products had not saved the life of a single peacekeeper.[40] On the other hand, multiple mission leadership teams have complained that insufficient PKI/SA strategic assets, such as long-range drones and ultra-high resolution mounted cameras, is a continual impediment to their understanding of their operating environment.[41] A survey of staff perceptions of the Unite Aware pilot in MINUSCA suggested that the technology was viewed as highly useful, though lacking a standardized mission-wide data architecture and integration with other tools and processes such as CPAS.[42] Some of the strongest endorsements of PKI/SA technologies come from instances in which there is a direct relationship between the situational awareness delivered by a sensor and an immediate tactical response, for example, the CCTV cameras that have been erected by MINUSCA in "hot spots" in the PK5 neighbourhood, or the mortar detection equipment in Kidal that alerts personnel to imminent threats.[43]

[38] Ibid.

[39] Adam Day, "Can Data Save U.N. Peacekeeping?", *World Politics Review*, 21 February 2019. Retrieved from https://www.worldpoliticsreview.com/articles/27479/can-data-save-u-n-peacekeeping.

[40] United Nations, "The All Sources Information Fusion Unit and the MINUSMA Intelligence Architecture: Lessons for the Mission and a UN Policy Framework," DPET/OMA/IOT internal report, UN Department of Peacekeeping Operations, 13 April 2016.

[41] Interviews with MINUSCA personnel, 8 and 22 May 2020.

[42] United Nations, "Interim Summary Report of the Lessons Learned Online Survey on the United Aware pilot roll-out in MINUSCA", DPET internal report, Department of Peace Operations, 1 June 2020.

[43] Interview with DOS/DMSPC personnel, 8 February 2021.

4. OPPORTUNITIES, CHALLENGES AND STRATEGIC QUESTIONS FOR THE FUTURE OF PKI/SA TECHNOLOGIES

a. Information requirements management and tasking

48. The immaturity of key mission-wide **peacekeeping-intelligence processes** across peacekeeping operations has been repeatedly emphasized by sensor operators and analysts as an impediment to the effective use of PKI/SA digital technologies. While most multidimensional missions have implemented some aspects of the DPO Peacekeeping-Intelligence Policy, such as the establishment of a mission PKI coordination mechanism or even the development of a mission-wide PKI acquisition plan, no mission has yet established a dynamic feedback loop between the intelligence products provided to decision-makers and articulation of their updated questions and requirements at a level of sophistication that would permit efficient tasking of different sensors across a mission.

49. Several challenges stand in the way of this. First and foremost, with some exceptions, most senior leadership in peacekeeping operations have yet to engage fully with peacekeeping intelligence processes. Some appear satisfied with the outputs of JMACs alone – which is perhaps not surprising, as SRSG's are JMACs' primary clients – while others appear unfamiliar with the PKI/SA capabilities at the mission's disposal or prefer to delegate such matters to the Force Commander. Personnel at the working level also suffer from a dearth of knowledge and expertise on intelligence cycle management, a mission-wide role that JMACs are meant to play but lack the resources to execute comprehensively. Efforts at DPO Headquarters to systematically recruit at least one career intelligence professional for each JMACs seeks to address this challenge while not fundamentally altering the character of JMACs.[44]

50. While the limitations of mission peacekeeping-intelligence cycles affect PKI as a whole, they are particularly detrimental to the use of digital PKI/SA technologies, which often have the capability to cover large geographic or informational spaces but can offer little without direction. In the absence of clear requirements from the mission, ISR units have resorted to "self-tasking", with unsatisfying results.[45]

b. Towards A.I., machine learning and predictive analysis

51. The Secretary-General's Data Strategy and the DPO PKI Policy both have as one of their core objectives **the strengthening of predictive** analysis to help missions and DPO strategize and plan. Indeed, the Data Strategy promises that effective data use will enable the UN to "forecast outcomes far more effectively than conventional techniques based on static historical reports."[46]

52. For peacekeeping's purposes, data-driven predictive analysis could contribute at two levels of analysis. First, within missions, the objective is to achieve what Allard Duursma and John Karlsrud term "**predictive peacekeeping**", wherein threat prediction can occur at a

[44] Interview, DPO personnel, 2 February 2021.

[45] Interview, former DPO personnel, 3 February 2021.

[46] United Nations, "Data Strategy for the Secretary-General for Action by Everyone, Everywhere, with Insight, Impact and Integrity", New York: Executive Office of the Secretary-General, p. 10.

sufficient level of detail and precision, and with sufficient warning to enable missions to plan and execute a response. Achieving such a state would, they argue, require achieving a much higher level of density and consistency in the Sage dataset or an alternative tool, and adding statistical modelling and/or machine learning techniques to supplant or complement more traditional qualitative scenario- or trend-based analysis. Event-based data could be complemented by big datasets already gathered in some missions, including social media and radio data.[47]

53. In addition to overcoming general challenges in the management of data discussed below, moving toward a more automated predictive event analysis system would need to address **cognitive and default biases** already present in peacekeeping data analysis event taxonomies. For example, a decision to reduce complexity in the MONUSCO Sage data entry form saw a large number of Mayi-Mayi groups collapsed into a single category for event perpetrator attribution, risking the identification of linkages where none exist.[48] Ongoing taxonomy debates have also highlighted the particular challenges of using value- and/or legally-laden terms, such as "terrorism" to describe events in a culturally and politically diverse analytical environment.

54. A second level of analysis for machine learning in peacekeeping could **analyze large amounts of data across missions** to deliver insights on best practices in mission responses, highlight outlying strategies, or compare and analyze peacekeepers' performance. Policy-driven analysis of this sort would require overcoming a general reticence among missions to release raw data to UN Headquarters. Missions cite the risk that data might be used absent sufficient context, or that politically sensitive information could be misinterpreted or released. While many of these questions have been at the core of the DPO data strategy for several years, the Secretary-General's data strategy has reinvigorated the agenda and provided higher-level direction, for example on plans to approximately triple the proportion of staff in the peace and security pillar in data-focused jobs to 10 per cent of the workforce by 2024.[49]

c. Authorities, limits, law and ethics

55. Information gathering in peacekeeping operations has always invoked ethical and human rights considerations about, for example, the security of sources, the provenance of information from security services, and protection of personally identifiable information. With the introduction of PKI/SA technologies to peacekeeping operations, the risks and challenges in this area have expanded exponentially and may have broad reputational and normative consequences.

56. The 2020 Peacekeeping-Intelligence, Surveillance and Reconnaissance (PKISR) military manual produced by the DPO Office of Military Affairs states that activities "must be conducted with full respect for human rights, including in particular the rights to privacy, freedom of expression, association and peaceful assembly and with particular care not to expose any sources or potential sources of information to harm."[50] It is unclear, however, what would constitute respect for human rights while operating PKI/SA technologies, particularly those with mass photographic or signals surveillance capabilities. Questions that arise in this

[47] Allard Duursma and John Karlsrud, "Predictive Peacekeeping: Strengthening Predictive Analysis in UN Peace Operations", *Stability: International Journal of Security and Development*, vol. 8, no. 1, pp. 1-19, 2019.

[48] Interview, DPO personnel, 28 January 2021.

[49] United Nations, "Data Strategy Update", slide deck, ICT Steering Committee, 22 January 2021.

[50] United Nations, "Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook (PKISR HB), First Edition", New York: UN Department of Peace Operations, September 2020, paragraph 2.1.3.

regard include what constitutes proportionality in the selection of surveillance objectives, where authorities for decision making on such questions lie, and what obligations missions have in terms of the protection of privacy and/or personally identifiable information, data retention and security, and oversight. While some TCCs/PCCs involved in the operation of PKI/SA technologies report that they are subject to national standards on these issues, these are often classified and, in any case, it is by no means clear that the UN would have the same interests and obligations as Member States, nor that standards would be the same across Member States.

d. An irreconcilable paradox of information ownership and sharing?

57. Uniformed peacekeepers have always been subject to their national doctrine and military/police frameworks. This is true both explicitly, in the sense that unis retain internal command structures, administrations, and disciplinary responsibility, and implicitly, in the sense that, in the absence of clear rules or guidance on a particular matter, it would be only natural to expect a unit to revert to its national doctrine. In a similar vein to the above trend, with the introduction of TCC/PCC-owned sensitive, complex digital technology systems into peacekeeping operations, national and UN legal, political and security frameworks have clashed in several ways that expose both the UN and TCCs/PCCs to legal and political risk. This challenge arises in several areas:

58. *Information ownership, custody and reach-back:* UN policy, rules and regulations clearly state that data and information gathered by UN peacekeepers are owned by the United Nations and its disposition the decision of the Secretary-General or his delegate. This clashes with legal obligations and operational security requirements of the TCCs/PCCs that deploy UNOE PKI/SA digital technologies in two ways. First, since some of the data produced by TCC/PCC sensors, such as telemetry data, is considered highly sensitive, this data is systematically removed during reach-back processing before being delivered back to the mission. While that information may be of no practical consequence, it means that the chain of custody is systematically broken. This leads to the second clash, which is that, during this break in the chain of custody, the disposition of the data is outside of the UN's oversight and control and yet within its responsibility and accountability. Anecdotal information suggests that, as a matter of standard national process, information being processed and analyzed enters national and, potentially, multinational databases, invoking the below concerns on information sharing.

59. *Transparency, oversight and accountability*: The use of sensitive digital surveillance technologies pose several novel challenges for the UN in articulating and ensuring a standard of transparency in its operations and in complying with principles and mechanisms of oversight and accountability expected by its legislative bodies. First, where classified TCC/PCC sensors and processes are used as part of a peacekeeping operation to acquire, process and analyze data, it appears impossible for the UN, Member States or the public to access information on the rules, techniques and strategies employed within the circle of TCC/PCC operational security. This, in turn, obscures the possibility that the UN could implement procedures for monitoring and enforcing compliance with standards of conduct for monitoring and surveillance, or establish mechanisms for persons in peacekeeping host-countries to bring grievances against peacekeeping missions concerning their surveillance activities.

60. *Information sharing and the Human Rights Due Diligence Policy*: Despite consensus in the Secretariat that the sharing of information constitutes "operational support" as defined in paragraph 7.e. of the UN Human Rights Due Diligence Policy on United Nations Support to non-United Nations Security Forces,[51] there does not appear to have been any serious attempt to date to understand the risks and – possibly – the observable consequences of the sharing of UN PKI/SA data and products with non-UN forces, including as a result of "reach-back."[52]

61. The PKISR handbook attempts to address some of the issues around the sharing of PKI/SA products or data by stipulating that any recipient of such materials must enter into a written agreement pledging that they will not be used in the commission of human rights violations and, moreover, that "attention should be paid to ensure their full compliance with the UN Human Rights Due Diligence Policy." In addition to being impractical where such information is shared automatically in the course of reach-back processing – for example with national or multinational databases – such guidance is flawed in that it puts the onus on the recipient to determine what could constitute a violation. In fact, the HRDDP requires that the provider of operational support – in this case, the mission – conduct a risk assessment of its own and make a determination on that basis.

e. Aligning management incentives to legal, political and ethical risk management for sensitive, intrusive surveillance technologies

62. In general, the procurement and deployment of PKI/SA technologies into peacekeeping operations have proceeded much the same as other information and communications technologies, in that operational support components of the Secretariat have largely managed these processes. With broad political support from senior UN leadership for the expanded use of technologies across the UN system, these capacities, which today have been consolidated into the shared DOS-DMSPC Office of Information and Communication Technology (OICT), have taken a leading role in identifying new technology solutions, building technology partnerships with Member States and suppliers through an "International Partnership for Technology in Peacekeeping" platform, and arranging the modalities for the receipt of new technologies in field operations.

63. While this arrangement may support technological innovation generally, it has created a serious legal, political and ethical blind spot when it comes to the acquisition of sensitive, intrusive surveillance technologies, with troubling implications. Risk management for the acquisition of these technologies has followed the same process as for standard procurement processes exercises, focused essentially on value for money and compliance with financial rules and regulations. Most processes appear to have largely excluded expertise on the legal, ethical, and human rights obligations and best practices for the use of surveillance equipment. Even within this standard process, it is not clear that any consideration has been given to whether providers of surveillance technologies – either through direct contracts or Letters of Assist – are in adherence with article 10 of the UN Supplier Code of Conduct, which states that suppliers are expected to support and respect the protection of internationally proclaimed human rights and to ensure that they are not complicit in human rights abuses. The document defines these abuses as violations of the principles derived from the Universal Declaration of Human Rights and set out in the United Nations Global Compact.[53]

[51] United Nations, A/67/775–S/2013/110, New York: UN General Assembly and UN Security Council, 5 March 2013.

[52] For a review of some of the risks related to information sharing in this context, see Olga Abilova and Alexandra Novosseloff, "Demystifying Intelligence in UN Peace Operations: Toward an Organizational Doctrine," New York: International Peace Institute, July 2016

[53] United Nations, "UN Supplier Code of Conduct Rev.06", New York: UN Procurement Division, December 2017.

f. Information security

64. In response to the increased sensitivity of some of the information it gathers, and the greater security exposure centralized digital storage brings, the UN has employed enhanced physical, technical and administrative measures for much if its data. Physically, the design of the MINUMSA secure network and the subsequent integration of components of the ASIFU into the U-2 has equipped the mission with some experience at secure cable and space management and generated a series of guidance and procedural documents that can be applied to future systems.[54] Technically, the report of the MINUSCA Unite Aware pilot lists measures taken to mitigate the risk of accidental or malicious misuse of data in the system, including measures to implement existing information management policy and guidance that is often otherwise ignored, as well as enhanced measures such as the maintenance of audit logs.[55] Administratively, OICT and DPPO/DPPA have invested in training and information campaigns in recent years to highlight good data management practices.

65. Despite these efforts, it seems reasonable to posit several assumptions about the innate limitation of UN cyber security and consider what this means for sensitive PKI/SA information storage and use. First, we can assume that the UN will be unable to prevent network intrusions from actors with the most sophisticated capabilities. Second, the splitting of allegiance involved by definition in the participation of uniformed personnel in peacekeeping means we can assume that it will be impossible to deter or manage away malicious misuse of data through training or trust alone. And, in any case, third, the UN's limited capacity to screen or grant security clearances means we can assume that the same reality applies to civilian personnel.

66. If these assumptions hold, it bears considering what this should mean for the UN's handling of sensitive data. Considerations could include the potential return to paper information handling in some cases, a maximalist approach to the management of access rights and logs, or perhaps limitations on what types of information to gather, or when to gather them. If missions are realistically unable to definitively protect sensitive information, should this cause the UN to reevaluate the value of centralized systems over the reliance on personal networks of sharing and trust that have dominated peacekeeping information-sharing environments for years?[56] As peacekeeping operations come to overlap with situations in which state-sponsored mis- and disinformation campaigns play out, as has been recently seen in the Central African Republic, it may be time to confront these assumptions more directly.

5. CONCLUSION

67. The diverse array of digital technologies for peacekeeping-intelligence and situational awareness inventoried in this paper make clear that these types of technologies now constitute a **key component of the technology portfolio**. As missions have strived to keep pace with the evolution of threats and the pace of technological change, the tools they deploy for these

[54] Interview 9 February 2021.

[55] United Nations, "MINUSCA Pilot: Unite Aware Implementation Project", End of Pilot Report, New York UN DOMSP Office of Information and Communication Technology, October 2019.

[56] For a detailed analysis of the role of trust in the management of peacekeeping-intelligence and its predecessors, see Sarah-Myriam Martin-Brûlé, "Competing for Trust: Challenges in United Nations Peacekeeping-Intelligence," *International Journal of Intelligence and Counter-Intelligence*, pp. 1-31, 2020.

purposes have become exponentially more powerful and complex. This paper's analysis of the capabilities, impact and challenges associated with PKI/SA technologies leaves us with three overall conclusions that could inform a new strategy for technology in peacekeeping.

68. First, PKI/SA technologies, especially surveillance technologies, constitute **a unique category of tools** within peacekeeping, and indeed within the Organization. Many of the more advanced and/or intrusive surveillance technologies deployed in peacekeeping operations in recent years pose considerable risks for human rights in their use as well as in the use of the information they generate. This reality does not disqualify them from use, but it does demand a tailored approach to the design, procurement and management of surveillance technologies that appropriately blends policy, political and human rights considerations with more traditional technology management practices. The Secretariat's current treatment of these technologies is much more akin to a "business as usual" approach and exposes the Organization to considerable legal, political, ethical, and operational risk.

69. Second, the impact of PKI/SA digital technologies will depend on **dramatically more consistent, structured and analytically appropriate data.** Moving beyond the important gains in short-term, tactical situational awareness brought by camp security technologies towards the goal of "predictive, data-driven analysis" and the potential application of machine learning will require further efforts to bring consistency in the volume and content of data entered across time and space in each mission. This is a very challenging task considering the diversity and rapid rotations of uniformed personnel, varying skills levels and available capacities across missions, and the complexity of the subjects being recorded. While considerable improvements have been made in recent years, a more transformative change will be required in the ubiquity of data gathering and entry will be required for tools like Sage or UniteAware to fully deliver on their goals. Along the way, DPO should be remain mindful that peacekeeping missions' qualitative analysis and insights developed by virtue of their proximity to the ground, relative legitimacy, and individualized analytical regimes are invariably the subject of envy among organizations with infinitely greater resources and technological capacities. Better quantitative analysis should not come at the expense of solid fieldwork and dogged inquiry.

70. Finally, the UN's host of technologies for monitoring, surveillance, information management, analysis and dissemination need to be understood and planned for as part of a **PKI/SA ecosystem** that blends technology, policy and practice. The purposes and use cases of individual technologies must be systematically defined in relation to PKI/SA policies and processes – notably, the peacekeeping-intelligence cycle – and in relation to one another. Despite an almost insurmountable constellation of competing institutional interests, some progress has been made in recent years to bring different tools and approaches closer together. However, in the absence of a definitive leadership vision and corporate decision-making, the inter-relations among these tools and approaches will continue to be decided in the bureaucratic trenches, with transaction costs that can be measured in terms of lost opportunities to improve effectiveness, efficiency and responsibility in peacekeeping. DPO and DOS are in dire need of unified, peacekeeping-wide leadership to define a vision for the PKI/SA ecosystem and adjudicate the respective roles of the tools, processes and practices within it.