Responsible Management and Use of Data in UN Peace Operations

Kseniya Oksamytna

OCTOBER 2023

Kseniya Oksamytna is a Senior Lecturer (Associate Professor) in International Politics at City, University of London and a Visiting Research Fellow within the Conflict, Security and Development Research Group at King's College London.

The author would like to express her sincere gratitude to Avishan Bodjnoud, Allard Duursma, Boukje Kistemaker, Sarah-Myriam Martin-Brûlé, Jenna Russo, Agathe Sarfati, and Albert Trithart for very helpful feedback on this and previous versions of the policy brief, as well as to Mariana Knaupp for skillful copyediting.

The views expressed in this paper represent those of the author and not necessarily those of the International Peace Institute. IPI welcomes consideration of a wide range of perspectives in the pursuit of a well-informed debate on critical policies and issues in international affairs. Any errors are the author's own.

IPI owes a debt of gratitude to its many donors for their generous support. This publication is part of IPI's Peacekeeping Observatory series, funded by the French Ministry of Armed Forces' Directorate General for International Relations and Strategy (DGRIS).

Executive Summary

With the increasing availability of diverse sources of information and sophisticated tools for its acquisition and analysis, UN peace operations face several challenges related to the responsible management and use of data. First, they may acquire data in ways that cause harm to those who provide the information. Second, they may rely too much on the most accessible types of data, such as information acquired from human sources or social media, leading to biased, incomplete, or erroneous assessments. Third, peace operations may create risks for civilians, peacekeepers, partners, or the UN's legitimacy if confidential data is accidentally disclosed. Finally, even when data is acquired and processed appropriately, it may not always feed into strategic analysis by mission leadership, UN headquarters, and the Security Council.

Recent efforts to standardize data acquisition, classification, reporting, and storage on platforms such as Sage and Unite Aware may be undermined by bureaucratic inertia, an absence of staff resources, or a lack of skills.[1] Procedures for the appropriate handling of data, especially data not stored in Sage or Unite Aware, are still in development. There are also many different systems for managing data across units in peace operations and other UN entities.

Building on recent progress in developing strategies and tools for the responsible and effective management and use of data, member states and senior UN leadership could consider the following recommendations:

- Improve the data-management skills of UN personnel;
- Strengthen the policy framework for the effective and responsible use of data;
- Provide adequate and predictable funding for data acquisition, analysis, and use;
- Enhance internal and external communication about the ways in which UN peace operations gather and use data; and
- Encourage the proactive use of data in strategic decision making.

1 Sage is an incident and event database used in peace operations to record developments related to mandate implementation. With the rollout of Unite Aware, Sage became an application in the Unite Aware suite called "Unite Aware Sage."

Introduction

In recent years, the UN has embarked on an ambitious project to use data more extensively and effectively to improve the safety of peacekeepers and the implementation of peace operations' mandates. This has included the rollout of new platforms for integrated analytics, such as Unite Aware. The increasing availability of various types of data in UN peace operations and the development of new tools for its acquisition and analysis present novel opportunities, enhancing peace operations' ability to predict and respond to violence; understand the population's sentiments towards peacekeepers; and provide better analysis to senior mission leadership, UN headquarters, and the UN Security Council.[2]

However, UN peace operations' greater use of data also presents challenges. For instance, information leaks can endanger the security of peacekeepers, as has already been the case with aerial operations in asymmetric environments. Additionally, irresponsible handling of a single image or name could cause serious harm to the reputation of peace operations, their beneficiaries, or member states.[3] When UN peace operations implement data-driven approaches that are not paired with the necessary data management capabilities and skills, they may be vulnerable to cyberattacks.[4] Both inappropriate data management or use and underutilization of data can cause harm. For example, if a mission collects but does not analyze data on threats to civilians or peacekeepers, it could fail in its responsibility to provide protection within its capabilities.

Both inappropriate data management or use and underutilization of data can cause harm.

This paper provides an overview of how UN peace operations acquire, process, manage, and use data in decision making; discusses UN policy frameworks on responsible data management; analyzes the challenges that peace operations face in acquiring, using, and disseminating data; and provides recommendations for member states, UN headquarters, and peace operations personnel on using and managing data more responsibly. The paper draws on document analysis and interviews with UN officials who work in peace operations and at UN headquarters.[5]

Types and Uses of Data in UN Peace Operations

It is necessary to consider all types of data with which peace operations work, including information that is useful for situational awareness, human rights violations data, and other kinds of information that relate to different aspects of peacekeeping mandates, such as information on local perceptions of the mission or the peace process.[6] Some of the data UN peacekeeping missions acquire and analyze is "peacekeeping-intelligence" (see Box 1).

Peacekeepers in practically every role generate or come across data that may be relevant to their mandates. Some sections in peace operations maintain databases specific to their remit—for example, databases on human rights violations for reporting to other parts of the UN system, such as the UN Security Council or the Office of the High Commissioner for Human Rights (OHCHR). Furthermore, peace operations officials may come across information that may enhance situational awareness even when they are not gathering peacekeeping-intelligence. For instance, in the course of their regular duties, an electoral affairs officer assisting with voter registration might receive information on pre-election tensions that pose a risk of violence.

2 On data-driven approaches to protection of civilians, see: Agathe Sarfati, "New Technologies and the Protection of Civilians in UN Peace Operations," International Peace Institute, September 2023.

3 As an official who has worked across a range of UN peacekeeping and political missions noted, "Just because there are pictures of one UN official with one disputable person, it can ruin decades of work." Interview with UN official, March 2021.

4 There have been allegations of cyberattacks against UN peace operations, which, despite being difficult to prove or disprove, point to the increased relevance of this threat for peacekeepers. "UN Peacekeeping Mission in Lebanon Says Its Data Protected by Strict Measures," *Economic Times*, June 30, 2022; Chloe FitzPatrick, "Cyber Peace: The Risks of IT Deployed to UN Peacekeeping Missions" (PhD dissertation, University of Queensland, 2021).

5 To respect the confidentiality of interviewees, no information is provided on their roles or ranks.

6 Data for reporting can be further disaggregated into two categories: data for reporting on developments in the host state and data for reporting on activities of the UN missions. On the latter, see: Daniel Forti, "UN Peacekeeping and CPAS: An Experiment in Performance Assessment and Mission Planning," International Peace Institute, October 2022.

Box 1. Types of peacekeeping-intelligence

Signals intelligence is obtained through the interception of signals, such as radio communication between members of armed groups.

Geospatial and imagery intelligence is obtained from satellites, closed-circuit television (CCTV) cameras, aircraft, unmanned aerial vehicles (UAV), remote sensors, or static sensors in mission area, such as tethered balloons or infrared sensors.

Information from human sources is acquired from people who have been directed to provide specific details about persons, incidents, or developments, in contrast to information the local population shares informally with members of peace operations during routine interactions.

Open-source intelligence comes from the media, including social media, the Internet, public events (such as political rallies or religious sermons), and public documents (such as leaflets or property records). Proprietary subscription-only datasets, such as Dataminr's First Alert, a service the UN subscribes to that provides information about natural and man-made disasters, are also considered open-source intelligence.

Technical intelligence is forensic analysis of material objects, such as the remains of improvised explosive devices (IEDs) that were denotated with the intent to harm peacekeepers or civilians.

In most contemporary multidimensional peacekeeping operations, several units play a role in acquiring, processing, and using peacekeeping-intelligence and other data. Military components of peacekeeping operations have a military intelligence branch known as U2. Civilian-led structures in charge of information gathering and analysis include the joint operations center (JOC) and the joint mission analysis center (JMAC).[7] JOCs and JMACs both include civilian, police, and military personnel, but they have distinct responsibilities.

The main tasks of JOCs are to provide 24/7 monitoring of the operational environment, consolidate information supplied by all mission components, produce daily reports for senior mission leadership and headquarters in New York, and act as a crisis-management center in emergency situations. For their part, JMACs offer mission leadership an analytical view of threats to mandate implementation.[8] In addition to these units, numerous other officials in UN peace operations—for example, protection of civilians advisers or human rights specialists—are also involved in handling information, which creates risks and opportunities for the responsible and effective management of data.

In theory, the UN has policies and guidelines on responsible data management and use in peace operations, including how to make them gender sensitive (see Box 2). However, the guidelines either lay down general principles for the entire UN in terms of working with data or focus on a specific peacekeeping-intelligence activity, such as acquisition of information from human sources or online (see Table 1 in Annex). There is a notable lack of guidance on how peace operations should work with data beyond peacekeeping-intelligence. Furthermore, the implementation of policies and guidelines is often hindered by constraints of human resources, skills, and the operational environment.

There is a notable lack of guidance on how peace operations should work with data beyond peacekeeping-intelligence.

7 A. Walter Dorn, "Intelligence-Led Peacekeeping: The United Nations Stabilization Mission in Haiti (MINUSTAH), 2006–07," *Intelligence and National Security* 24, no. 6 (2009), 805–835; Olga Abilova and Alexandra Novosseloff, "Demystifying Intelligence in UN Peace Operations: Toward an Organizational Doctrine Intelligence," International Peace Institute, July 2016.

8 Allard Duursma, "Counting Deaths While Keeping Peace: An Assessment of the JMAC's Field Information and Analysis Capacity in Darfur," *International Peacekeeping* 24, no. 5 (2017), 823–847.

Box 2. Gender, data, and UN peace operations

Gender can affect all aspects of data acquisition, management, and use in peace operations. At the data-acquisition stage, the presence of male or female peacekeepers can constrain or enhance the mission's ability to engage with sources. This is one of the justifications for the UN's deployment of United Nations Engagement Platoons (UN-EPs), which are gender-balanced teams seen as more likely to acquire accurate peacekeeping-intelligence and situational awareness information.[9] For instance, Indian women peacekeepers in the UN Interim Security Force for Abyei (UNISFA) were invited into the homes of young girls in the village they visited, something that all-male peacekeeper teams did not experience.[10] Such encounters can enhance opportunities for acquiring relevant information. At the data-management stage, the conversion of raw data into information that can be useful for mandate implementation can be affected by gender biases, as evaluators of different genders are likely to highlight, discard, and interpret information differently. At the data-use stage, decision makers may be inattentive to gender biases in data. For example, women's more limited access to technological tools and platforms may affect the usability of open-source intelligence, which can in turn affect the quality of decisions by UN personnel.

The UN is making efforts to ensure that its procedures for acquiring, managing, and using data are gender-sensitive. While gender used to be an overlooked aspect of policy development and practice related to peacekeeping-intelligence, there has been a considerable effort to address this issue.[11] For example, the Guidelines on Acquisition of Information from Human Sources for Peacekeeping-Intelligence stipulate that engagement with human sources should take place when at least two UN personnel are present, and a mixed-gender team is ideal. The guidelines stress that the risk assessment prior to the engagement should weigh whether either the peacekeeper or the source might face threats or be subjected to reprisals, including because of their gender. They also challenge gendered stereotypes of women as passive victims of armed conflict or "natural peacemakers," emphasizing the need to pay attention to women who may be members of armed groups. Additionally, the guidelines remind that in gathering information on sexual violence, peacekeepers should remember that men, not only women, can be survivors and should consequently make inquiries about people of all genders. The guidelines provide a comprehensive list of gender-responsive indicators that analysts should take into account, such as gendered narratives for recruitment into armed groups, breakdowns of marriage negotiations, or changes in social norms around dress.

Overall, the guidelines stress the importance of (1) identifying how conflict affects people of different genders and how data reflects that, (2) understanding how gender affects drivers of conflict and peace, and (3) enabling senior mission leadership to make gender-responsive decisions to enhance the protection of both peacekeepers and civilians.[12]

9 UN Peacekeeping, "United Nations Engagement Platoon Handbook: First Edition," October 18, 2022.

10 Annalysse Mason, "Action for Peacekeeping: Engagement Platoons Champion Gender Parity in Peacekeeping and Beyond," UN Peacekeeping, March 24, 2023, available at https://peacekeeping.un.org/en/action-peacekeeping-engagement-platoons-champion-gender-parity-peacekeeping-and-beyond .

11 Sarah-Myriam Martin-Brûlé, "Finding the UN Way on Peacekeeping-Intelligence," International Peace Institute, April 2020.

12 UN Department of Peace Operations (DPO), "Guidelines: Acquisition of Information from Human Sources for Peacekeeping-Intelligence," September 1, 2020.

Responsible Data Acquisition, Use, and Dissemination in UN Peace Operations

At the stages of data acquisition, use, and dissemination, UN peace operations may encounter challenges related to data protection and quality. Data protection is necessary to ensure that peacekeeping missions do not cause unintended harm by disclosing sensitive or personal information and that aggregated data acquired by the UN is not used for planning or committing human rights violations. For example, aggregate data patterns may expose ethnic or social groups to targeted attacks.[13] In turn, data quality is essential for the UN to meet its responsibilities to member states, including host governments. Analysis based on erroneous or incomplete data may prevent missions from effectively protecting civilians or implementing other aspects of their mandate.

> When acquiring information from the operational environment, UN peace operations need to be mindful of four ethical principles: the "do no harm" approach, data protection, data ownership, and data quality.

Data Acquisition

When acquiring information from the operational environment, UN peace operations need to be mindful of four ethical principles: the "do no harm" approach, data protection, data ownership, and data quality. First, the "do no harm" approach entails making sure that peacekeepers do not make the population worse off than it would be if the mission were not present. For example, civilians who engage with peacekeepers, usually in public spaces like markets or municipal buildings, can be identifiable by hostile parties, and peacekeepers need to manage this risk.[14] They have not always done so effectively, however.

For example, the UN Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO) organized community alert networks by providing participating civilians with new phones or radios.[15] This posed three issues. First, civilians who collaborated with the mission stood out in their communities and thus were visible to hostile parties. Second, the provision of new phones or radios to a select few exacerbated inter- and intracommunal tensions. Third, there was a risk that the provision of phones or radios could serve as a perverse incentive for civilians to participate in the network even if they were not well placed to provide early warning. MONUSCO subsequently shifted to more discreet communication channels, such as toll-free hotlines or prepaid SIM cards for focal points selected by communities themselves.[16]

In the UN Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), the community alert network model was not feasible, as civilians feared reprisal attacks for participating. Instead, MINUSMA established toll-free hotlines in all its regional offices.[17] However, it took the mission two years to establish this hotline due to political challenges: the host government was slow to give approval, and telecommunications operators were wary about collaborating with MINUSMA, anticipating the government's potential reaction.[18]

In general, UN policy specifies that information from human sources should only be considered when "acquisition of the necessary information from other sources has proven impossible or inconclusive."[19] In practice, however, gathering

13 Allard Duursma and John Karlsrud, "Predictive Peacekeeping: Strengthening Predictive Analysis in UN Peace Operations," *Stability* 8, no. 1 (2019), 1–19.

14 Allard Duursma, "Information Processing Challenges in Peacekeeping Operations: A Case Study on Peacekeeping Information Collection Efforts in Mali," *International Peacekeeping* 25, no. 3 (2018), 446–468.

15 Harley Henigson, "Community Engagement in UN Peacekeeping Operations: A People-Centered Approach to Protecting Civilians," International Peace Institute, November 2020.

16 Prepaid phone cards are not considered incentives but reimbursement for expenses that local actors incur by virtue of providing information to the mission. UN Peacekeeping, "MONUSCO: Protection of Civilians and Protection Tools," available at https://monusco.unmissions.org/en/protection-civilians-and-protection-tools .

17 Seán Smith, "Early Warning and Rapid Response: Reinforcing MINUSMA's Ability to Protect Civilians," Center for Civilians in Conflict (CIVIC), April 2021.

18 Interview with former UN official, September 2023.

19 UN DPO, "Guidelines: Acquisition of Information from Human Sources for Peacekeeping-Intelligence," p. 6.

information from human sources remains an important method of improving situational awareness, including through the community alert networks and toll-free hotlines discussed above. The Cruz report argues that building networks of informants should be prioritized to enhance peacekeepers' safety, an example of the disconnect between UN policy and operational realities.[20]

The second ethical challenge that arises during data acquisition relates to data protection. Different units in peace operations vary in the extent to which they prioritize data privacy and security. For example, human rights units, which often have lawyers among their staff, have robust procedures, methodologies, and training for engagement with civilians and observe stringent standards for source and witness protection.[21] Yet JMAC officials, who maintain an extensive network of contacts to obtain, verify, and understand information, may not be trained in the conventional military or legal aspects of intelligence gathering.[22] The May 2023 update of the Policy on the Protection of Civilians in United Nations Peacekeeping reminded JMAC personnel of the need to "ensure an appropriate level of confidentiality in the acquisition, handling and sharing of information (including source protection), and the appropriate dissemination of final products."[23]

The third ethical challenge associated with data acquisition in peace operations is data ownership. Individuals should be able to exercise rights regarding data collected about them, including the right to withhold or withdraw information.[24] In UN peace operations, however, these rights can be difficult to uphold due to the long chain of delegation. A mission exercises its right to acquire information based on the consent of the host government and the UN Security Council resolution mandating its presence. For example, the ethical implications of the CCTV cameras installed by the UN Multidimensional Integrated Stabilization Mission in the Central African Republic (MINUSCA) in a crime-affected neighborhood of Bangui are unclear, as Central African civilians have limited means to complain about or object to the mission's surveillance activities.[25] The perceived lack of transparency around how and for what purposes peace operations acquire information may damage trust in the mission. For instance, when unmanned aerial vehicles (UAVs) were first introduced to peacekeeping, humanitarian actors warned that the population would not know whether these UAVs were armed or not, creating a risk of further traumatizing civilians living through conflict.[26]

Individuals should be able to exercise rights regarding data collected about them, including the right to withhold or withdraw information.

Finally, missions may be unable to acquire high-quality data in all regions where they work. Geospatial and imagery intelligence may be less useful in forested areas than in plains or deserts and can also be hampered during bad weather.[27] This may disadvantage civilians who live in or around particular areas where foreign and local armed groups operate, such as the Garamba National Park in northeastern Democratic Republic of the Congo (DRC).[28] Open-source data, such as data acquired through the analysis of social media or community radio broadcasts, presents a different set of quality

20 Carlos Alberto dos Santos Cruz, "Improving Security of United Nations Peacekeepers," UN Peacekeeping, November 2017.

21 Interview with UN official, May 2023. On how different sections in a peacekeeping operation approach the mandate, see: Kseniya Oksamytna, Oisín Tansey, Sarah von Billerbeck, and Birte Julia Gippert, "Theorizing Decision-Making in International Bureaucracies: UN Peacekeeping Operations and Responses to Norm Violations," *International Studies Quarterly*, forthcoming.

22 Lauren Spink, "Data-Driven Protection: Linking Threat Analysis to Planning in UN Peacekeeping Operations," CIVIC, November 2018; Martin-Brûlé, "Finding the UN Way on Peacekeeping-Intelligence."

23 UN DPO, "Policy: Protection of Civilians in United Nations Peacekeeping," May 1, 2023.

24 Richard Heeks and Jaco Renken, "Data Justice for Development: What Would It Mean?" *Information Development* 34, no. 1 (January 2018), 90–102.

25 Dirk Druet, "Enhancing the Use of Digital Technology for Integrated Situational Awareness and Peacekeeping-Intelligence," UN DPO, April 2021. CCTV cameras have been used in peacekeeping since 2008, but in contexts less likely to raise ethical concerns—for example, monitoring the buffer zone in Cyprus. A. Walter Dorn, "Electronic Eyes on the Green Line: Surveillance by the United Nations Peacekeeping Force in Cyprus," *Intelligence and National Security* 29, no. 2 (2013), 184–207.

26 Sophie Pilgrim, "Are UN Drones the Future of Peacekeeping?" *France24*, April 9, 2015.

27 Elodie Convergne and Michael R. Snyder, "Making Maps to Make Peace: Geospatial Technology as a Tool for UN Peacekeeping," *International Peacekeeping* 22, no. 5 (2015), 565–586.

28 On the difficulties of operating in such terrain, including those related to situational awareness, see: Paul D. Williams, "How Peacekeepers Fight: Assessing Combat Effectiveness in United Nations Peace Operations," *Security Studies* 32, no. 1 (2023), 32–65.

issues, especially in terms of coverage and bias.[29] In most countries hosting peacekeeping missions, a minority of the population has access to the Internet and social media, and this percentage is even smaller in areas that are remote or experiencing instability. Relying excessively on open-source intelligence may leave UN personnel with a poor understanding of the security concerns of such populations.[30]

Furthermore, access to the Internet or the ability to phone in to community radio stations varies by gender and socioeconomic status. Additionally, self-censorship and government-imposed restrictions on freedom of speech are widespread in conflict-affected environments, affecting, for instance, information that community radio stations are able to broadcast.[31] For these reasons, UN personnel need to keep in mind the limitations of various methods of data acquisition.

Data Processing and Storage

UN peace operations acquire a large amount of information but may not have the capabilities to process it.[32] Despite ongoing attempts at centralization and standardization, various sections in peace operations, as well as other UN entities, maintain separate databases.[33] Military components use the i2 database. Human rights units feed information into the OHCHR database of human rights violations. Child protection units maintain a database on violations of children's rights for the monitoring mechanism on grave violations committed against children in armed conflict. The UN Department for Safety and Security (UNDSS) operates a Safety and Security Incident Reporting System (SSIRS) in all countries where the UN has presences, including peace operations.[34] The UN Mine Action Service (UNMAS) has its own global information-management system, which contains information on threats of mines and explosive remnants of war.[35] Public information and strategic communications officials monitor traditional and social media, recording and storing the data in their own ways.[36] While the integration of these databases might not be possible or even desirable, data-governance procedures are needed to ensure the information contained in the databases is fully utilized in the decision-making process.

> Units in peace operations differ in the extent to which they protect data that they send to JOC for processing.

Units in peace operations differ in the extent to which they protect data that they send to JOCs for processing.[37] In MINUSMA, human rights sections provided only sanitized data that did not contain any personal information on witnesses or survivors; by contrast, daily reports from the military component contained names, contact details, and physical descriptions of civilians with whom patrols interacted. These reports were sent to JOC by email.[38] While the UN sought to increase the security of its email communications by introducing multi-factor authentication, data transmission remained vulnerable to cyberattacks, as well as unauthorized disclosure due to human error or co-optation.

Although such portrayals risk exacerbating biases against some categories of UN personnel, the UN Military Peacekeeping-Intelligence Handbook singles out several categories of individuals who

29 For a discussion of a MINUSMA pilot to mine data from community radio broadcasts, see: Stefan Lemm, "Data Privacy and Protection Assessments in Radio Mining," UN Office of Information and Communications Technology (OICT), April 12, 2021.

30 For a conceptualization of the right of data representation or inclusion (a right to be represented in datasets), see: Heeks and Renken, "Data Justice for Development."

31 Apryl Williams and Benjamin K. Tkach, "Access and Dissemination of Information and Emerging Media Convergence in the Democratic Republic of Congo," *Information, Communication & Society* 25, no. 10 (2022), 1383–1399.

32 Eleonore Pauwels, "Peacekeeping in an Era of Converging Technological and Security Threats: Preventing Collective AI and Data Harms, Learning to Save Lives with Dual-Use Technologies," UN DPO, April 2021; A. Walter Dorn and Cono Giardullo, "Analysis for Peace: The Evolving Data Tools of UN and OSCE Field Operations," *Security and Human Rights* 31 (2020), 90–101.

33 Martin-Brûlé, "Finding the UN Way on Peacekeeping-Intelligence"; Allard Duursma, "Mapping Data-Driven Tools and Systems for Early Warning, Situational Awareness, and Early Action," PAX, April 2021.

34 Druet, "Enhancing the Use of Digital Technology."

35 Interview with UN official, May 2023.

36 Druet, "Enhancing the Use of Digital Technology"; Albert Trithart, "Disinformation against UN Peacekeeping Operations," International Peace Institute, December 2022.

37 All sections transmit daily reports to JOCs, often to their subnational offices, to be collated and presented to the mission leadership and UN headquarters.

38 Interview with UN official, May 2023.

may pose a risk of unauthorized information disclosure, such as national staff, locally recruited contractors, and interpreters.[39] In MINUSMA, whose aerial assets were targeted by hostile elements that sought to prevent patrols, an information leak was discovered when several flights were disrupted by successful or attempted attacks, despite the mission's efforts to change flight schedules every week. There was a possibility that the leak was due to national staff taking note of the mission's flight schedules and transferring this information to outside actors.[40] At the same time, if UN training materials and security procedures present all national staff as a constant security threat, these staff may suffer the demoralizing effect of being suspected of disloyalty to the organization.[41] This is especially important because many information-analysis units, such as JMACs, characterize national staff as indispensable to their work.[42]

To help combat the difficulties JOCs face in collating vast amounts of information, the UN introduced Sage, a database where military, police, and civilian officials can log, categorize, and systematize incidents and events. Most peacekeeping operations and some special political missions currently use the database.[43] JOCs, as well as military and police components, have access to tools on Sage for managing confidential information, such as personal data of individuals involved in security incidents, which members of other components cannot view unless they have additional authorization. Users with Microsoft PowerBI skills and the necessary permissions can use Sage datasets to produce dynamic dashboards visualizing hotspots of violence or other activity. However, missions rarely have enough officials with the necessary data analytics skills.[44] The advantage of Unite Aware is that it incorporates dashboards for everyone in the mission to use, which can in part address this issue.

JOCs are responsible for ensuring that data in Sage is accurate and complete, but maintaining data quality has been a persistent challenge.[45] In MINUSMA, each subnational JOC followed its own approach in counting the number of actors affected by each incident, with some JOCs counting only survivors of violence and others adding perpetrators. To give another example, some subnational JOCs classified irrelevant developments, such as peaceful demonstrations, as protection of civilians incidents, without recording others, such as the intimidating presence of armed actors.[46] After UN headquarters requested around late 2022 that the military and police components engage with Sage instead of relying on their own databases, MINUSMA took action to improve data verification and consolidation, making Sage data more reliable. A committee chaired by JOC, consisting of representatives of the U2, JMAC, protection of civilians specialists, and sometimes UN police, met three times a week to verify inputs into Sage. Yet even in JOC, some officials lacked the necessary data-management skills, particularly military officers seconded to JOC for six-month tours. The field technology section offered in-mission training, but section heads could not release their staff to the two-day session due to resource constraints.[47]

In some missions, inadequate staffing has meant that the responsibility for information management has fallen to UN volunteers, who lack the seniority and permanence to initiate large-scale improvements to data-management processes.[48] Another indicator of limited staff capacities was that in MINUSCA, Norway financed a JOC opera-

39 United Nations, "Military Peacekeeping-Intelligence Handbook," April 22, 2019.

40 Interview with former UN official, September 2023.

41 UN General Assembly, *Evaluation of the Organizational Culture in Peacekeeping Operations: Report of the Office of Internal Oversight Services*, UN Doc. A/75/803, March 8, 2021; Katharina P. Coleman, "Downsizing in UN Peacekeeping: The Impact on Civilian Peacekeepers and the Missions Employing Them," *International Peacekeeping* 27, no. 5 (2020), 703–731.

42 Martin-Brûlé, "Finding the UN Way on Peacekeeping-Intelligence."

43 UN Doc. A/75/803.

44 Interview with UN official, May 2023.

45 See also: Marion Laurence, "What Are the Benefits and Pitfalls of 'Data-Driven' Peacekeeping?" Center for International Policy Studies, December 2019, available at https://www.cips-cepi.ca/wp-content/uploads/2020/01/policy-brief-marion-laurence-1.pdf .

46 Melanie Sauter, Sebastian Frowein, and Marcello Cassanelli, "A Data-Driven Tool to Advance the Protection of Civilians During Force Operations," MINUSMA Protection of Civilians Unit (2020), on file with author.

47 Interview with UN official, May 2023.

48 Interview with UN official, May 2023.

tions officer (a P4 authorized to act as deputy head of JOC) through extrabudgetary contributions.[49]

For these reasons, enthusiasm for new data tools at UN headquarters might not be shared universally across missions that struggle with day-to-day challenges.[50] UN headquarters might prioritize the acquisition of data through new tools over allocating resources to assess its quality and provide guidance for how it is supposed to be used. This disconnect between headquarters and the field may undermine the effective utilization of the new and more advanced data-management platform Unite Aware. The platform, championed by India, integrates patrol planning, incident reporting, real-time asset tracking, and multilayer mapping tools.[51] Following a pilot in MINUSCA completed in October 2019, Unite Aware was fully implemented in the UN Peacekeeping Force in Cyprus (UNFICYP) in January 2023.[52] As part of the Unite Aware rollout, the UN Situational Awareness Programme, a joint initiative of the UN Department of Peace Operations (DPO) and the Office of Information and Communications Technology (OICT), deployed system and business analysts to codesign the digital transformation process. After the rollout of Unite Aware was completed, a business analyst and data expert stayed in the mission to aid with the integration of these new capabilities. This included the creation and facilitation of a Data Governance Working Group representing most mission sections. Consequently, gradual changes to Unite Aware applications were introduced to improve data collection and sense-making, as well as facilitate data-driven briefings.[53]

However, the introduction of Unite Aware is likely to proceed differently depending on each mission's mandate, its operational environment, and the support it receives for this endeavor.[54] The situation is complicated by the multitude of actors supporting peace operations' data acquisition and management.[55] Sage is maintained by the UN Operations and Crisis Centre (UNOCC), while the entity charged with maintaining Unite Aware is unconfirmed. Training on the use of Sage and Unite Aware, including relevant security procedures, is provided by the OICT. Support on all other aspects of mandate implementation, as well as policy development on data acquisition and management, is provided by DPO and the Department of Political and Peacebuilding Affairs (DPPA) for peacekeeping and special political missions, respectively. Due to this disjointed system of governance, training, and backstopping, users of the platform might be unsure where to obtain assistance and direction.

Many officials, such as political affairs officers, civil affairs officers, and gender advisers, come in contact with personal and sensitive data without clear guidance on what procedures to follow to protect it.

If information does not relate to security incidents, which are logged into either Sage or Unite Aware, it may not be perceived as warranting specific protection. However, many officials, such as political affairs officers, civil affairs officers, and gender advisers, come in contact with personal and sensitive data without clear guidance on what procedures to follow to protect it (human rights officers are an exception, as discussed above). As one UN official admitted, the UN's data-storage systems "are a sieve."[56] The main platform for sharing non-incident-related information is Microsoft SharePoint, which has procedures in place for data security and protection. Therefore, missions have been encouraged to move away from Word, Excel, and email-based exchanges "to more SharePoint-based information-management structures to make it more robust, so it cannot be tampered with, intentionally or unintentionally."[57] Still, some officials see

49 UN Talent, "JOC Operations Officer, MINUSCA, Bangui, P4, NORDEM," 2022, available at https://untalent.org/jobs/joc-operations-officer-minusca-bangui-p4-nordem .

50 Interview with UN official, May 2023.

51 "India in Collaboration with UN Launches Tech Platform for Peacekeepers," *Times of India*, Aug 18, 2021.

52 UN Peacekeeping, "Action for Peacekeeping Digital Transformation Underway in UNFICYP," January 2, 2023.

53 Interview with former UN official, July 2023.

54 There had been plans to introduce Unite Aware in MINUSMA before the host government's request for the mission's withdrawal in June 2023.

55 Druet, "Enhancing the Use of Digital Technology."

56 Interview with UN official, June 2023.

57 Interview with former UN official, July 2023.

SharePoint as insufficiently secure and avoid using it for storing important documents or data.[58] This can lead to data hoarding as a consequence of data storage on personal devices. Frequent intra-mission disagreements on how to classify data can be another reason behind data hoarding.

UN personnel's preference for keeping data on personal devices poses another security risk. Unencrypted personal devices, such as smartphones or flash drives, are vulnerable to hacking or theft, which might endanger the personal data of local contacts.[59] This may also lead to data loss when officials leave the mission. In general, due to the perceived absence of accountability for the handling of data, officials in peace operations might be lax with data privacy and protection because they think they can afford to be.[60]

> Ultimately, the goal of data generation by missions is to inform strategic decision making by mission leadership, UN headquarters, and the UN Security Council.

Data Use, Analysis, and Dissemination

The final step in using data in peace operations is its analysis and, in some cases, dissemination. At this stage, the main concern is how to use data in a way that avoids unintended harm and enhances operations' ability to implement their mandates. For instance, a persistent issue with information acquired from human sources is its unreliability. In MONUSCO, overreliance on a single human source of information might have misinformed strategic-level decision making. After a self-proclaimed commander from the Allied Democratic Forces (ADF) surrendered to MONUSCO, his testimony might have led to an exaggeration of the threat the group posed and an incomplete view of its motives, although national MONUSCO staff and Congolese NGOs doubted the credibility of the information.[61] Conversely, in MINUSMA, the military component tended to distrust information acquired from human sources due to a belief that the reported threats were exaggerated and concern that deliberately misleading information could lead to an ambush.[62] Triangulating information acquired from human sources with data obtained in other ways, such as through social media monitoring, might be a partial remedy, although correct interpretation of any information requires careful judgment by mission leadership and relevant officials.

Crucially, in terms of data analysis, there are questions about what information is provided to senior mission leadership and how often. While JOCs transmit a daily summary to senior mission leadership, it is usually based on data from Sage and Unite Aware, and there are issues with data quality and differences in how to classify incidents, as discussed above. Furthermore, a detailed log of every incident might not be of much use to mission leaders who need an overview of the overall security situation and political process. While JMACs report on medium- and long-term trends, drawing on data generated by all mission sections and JMAC itself, it is unclear whether all units provide JMACs all the information they have. They also may not provide this information in useful formats, in contrast with the established routines for entering information into Sage and Unite Aware. In some cases, this might be due to unclear communication from JMAC and senior mission leadership about missions' data needs.

Nonetheless, there are examples of missions effectively analyzing and using data. For instance, when data collected and analyzed by UNFICYP revealed that seasonal agricultural activities tended to result in more incursions into the buffer zone that separates the Republic of Cyprus and

58 Interview with UN official, June 2023.

59 Officials in peace operations store sensitive information on flash drives, and some have only recently considered encrypting them. Interview with UN official, June 2023.

60 Interview with UN official, June 2023.

61 Kristof Titeca and Daniel Fahey, "The Many Faces of a Rebel Group: The Allied Democratic Forces in the Democratic Republic of Congo," *International Affairs* 92, no. 5 (2016), 1189–1206.

62 Seán Smith, "Early Warning and Rapid Response."

the Turkish Republic of Northern Cyprus, the mission and other parties engaged in contingency planning to minimize tensions during the following season.[63] Data can also be transmitted to third parties for analysis. For example, UNOCC has a partnership with the AI Centre and Institute for Machine Learning at ETH Zürich to analyze aggregate data patterns from Sage. The aim of this project is to assess whether artificial intelligence (AI) and machine-learning tools can assist peace operations with early warning.[64] Sage data provided to ETH is stored in LeoMed, a secure platform to transfer, store, manage, and analyze sensitive research data. As the number of similar partnerships increases, the UN is likely to consider developing policy frameworks regulating issues around data privacy, security, and data ownership in such cases.

Ultimately, the goal of data generation by missions is to inform strategic decision making by mission leadership, UN headquarters, and the UN Security Council. In July 2023, data visualizations from missions' own data-management systems were used in the secretary-general's report to the UN Security Council. The report on UNFICYP presented figures from Unite Aware on the number of civilian, military, and criminal incidents in the buffer zone, as well as figures from the Comprehensive Planning and Performance Assessment System (CPAS) on mission-facilitated information exchanges between the parties to the conflict.[65] These practices demonstrate to all member states the added value of investments in data acquisition and management by peace operations.

The use of AI and machine learning in peace operations also poses opportunities for more effective analysis. For instance, machine-learning algorithms for extracting data from multiple sources of unstructured content for automated inclusion in Sage or Unite Aware could reduce the need for the manual logging of incidents and free up JOC resources to focus on data compilation and verification.[66] However, while the 2022 Principles for the Ethical Use of Artificial Intelligence in the United Nations System stress the importance of adequate data-protection frameworks and data-governance mechanisms, guidelines on the use of AI and machine learning in peace operations have not yet been developed.[67]

> In general, when missions report on their activities, they should pay more attention to protecting the identities of partners and beneficiaries, as well as of mission officials themselves.

Finally, some ways in which peace operations disseminate information may compromise data security and privacy. For example, the geographic information system (GIS) section of the UN Mission in South Sudan (UNMISS) produced a map with the locations of quick-impact projects financed or implemented by the mission. However, this map revealed the names of the implementing partners, sometimes including photographs of the individuals involved.[68] In environments where a peace operation is not perceived as an impartial actor, identifying mission partners in this way could put them at risk.[69] When developing memoranda of understanding (MOUs) with quick-impact project implementing partners, missions need to make sure these partners provide informed and voluntary consent to the dissemination of data in such a manner, in addition to carefully weighing the benefits of publicity against privacy and security risks.[70]

63 Interview with former UN official, July 2023.

64 Allard Duursma, "Data-Driven Analyses in UN Peace Missions," March 13, 2022.

65 UN Security Council, *United Nations Operation in Cyprus: Report of the Secretary-General*, UN Doc. S/2023/498, July 5, 2023. The report also presented a figure on asylum applications in the Republic of Cyprus from the UN High Commissioner for Refugees.

66 Interview with UN official, July 2023.

67 UN System Chief Executives Board for Coordination, "Principles for the Ethical Use of Artificial Intelligence in the United Nations System," September 20, 2022.

68 UN Peacekeeping, "UNMISS Quick Impact Projects Map," 2018, available at https://unmiss.unmissions.org/unmiss-quick-impact-projects-map .

69 Kseniya Oksamytna, Lisa Hultman, Charlie Hunt, Dennis Gyllensporre, Marco Donati, and Allard Duursma, "Protection of Civilians," in "UN Peacekeeping at 75: Achievements, Challenges, and Prospects," *International Peacekeeping*, forthcoming.

70 For a discussion of ethical issues surrounding quick-impact projects, see: Kseniya Oksamytna, *Advocacy and Change in International Organizations: Protection, Communication, and Reconstruction in UN Peacekeeping* (Oxford: Oxford University Press, 2023), Chapter 5; and Melanie Sauter, "A Shrinking Humanitarian Space: Peacekeeping Stabilization Projects and Violence in Mali," *International Peacekeeping* 29, no. 4 (2022), 624–649.

In general, when missions report on their activities, they should pay more attention to protecting the identities of partners and beneficiaries, as well as of mission officials themselves. For example, when the names of national staff members are disclosed on a mission's website, it could make them and their families targets of harassment by government security forces or armed groups that view the mission with hostility. While national staff members are known in their communities, they might not be known to armed actors from a different region or to a foreign armed group, and identifying information should therefore be disseminated with caution.

In terms of public information and strategic communications products such as posters and newsletters, peacekeepers need to ensure that they do not disseminate information that could harm the communities where they work. For example, missions often highlight the psychosocial or socio-economic assistance they render to survivors of sexual violence. When they do this, they should use names and photographs of beneficiaries only after conducting a proper risk assessment and only with the voluntary and informed consent of the survivors to avoid exacerbating the discrimination they face. Missions should exercise special care when minors are involved. Even in internal reporting to headquarters, missions should avoid disseminating sensitive or personal data, considering that reports may be shared with member states that have relations with various parties to the conflict.

Conclusion and Recommendations

The UN has invested considerable effort into developing policy frameworks for managing data in peace operations. Various strategies, policies, and guidelines stress the importance of data privacy, security, and quality, as well as the need to prevent accidental harm to peacekeepers and civilians in the process of acquiring, processing, storing, analyzing, and disseminating data, although coherence between these documents could be further improved.

At the same time, missions face challenges in terms of the responsible and effective management and use of data. Peace operations may expose their sources to accidental harm if those sources are identifiable to hostile or repressive actors. Novel surveillance technologies, such as CCTV or UAVs, may cause suspicion among the local population. Data that peace operations acquire might be of uneven quality, and it may be stored in disjointed systems maintained by different mission units or parts of the UN system. Recent efforts at systematizing data on platforms like Sage or Unite Aware have shown promising results, but missions differ in how effectively they use those platforms. SharePoint is being promoted as a more secure alternative to email-based collaboration on documents, but some personnel are disinclined to use it, resulting in data hoarding or insecure data storage.

There are several ways in which member states, UN headquarters, and peace operations personnel can use and manage data more responsibly:

Improve the data-management skills of UN personnel: Data literacy of UN personnel remains a serious challenge. Cataloguing, handling, analyzing, and communicating data correctly and securely requires expertise and experience. This could be achieved by improving all personnel's ability to work with data extracted from Sage, Unite Aware, or other databases. The UN plans to fund three training-of-trainer workshops on Unite Aware in 2024 and 2025 for civilian and uniformed personnel with the expectation that the skills would eventually be disseminated widely across missions. This complements the existing provision of online training through the C4ISR Academy for Peace Operations, which is oriented primarily toward training uniformed peacekeepers in the so-called C4ISR technologies (UN command, control, communications, computers, intelligence, surveillance, and reconnaissance) but also offers online courses to civilian peace operations staff. Such initiatives should be scaled up and sped up. The UN is also planning to train senior mission leadership in how to use data and information to support decision making, as well as in data governance and management. For all personnel, there is training

71 UN Peacekeeping, "Pledging Guide for the 2023 United Nations Peacekeeping Ministerial," May 22, 2023.

planned on data ethics and privacy, data analysis, data visualization, and data retention.[71] Such training should be tailored to the needs and workload constraints of officials in each mission.

Lack of appropriate skills is compounded by frequent rotations of personnel, both uniformed and civilian. Member states should consider extending the rotations of uniformed personnel in key data-handling roles and put forward candidates with strong data skills, while UN headquarters should improve the hiring, retention, and upskilling of civilian staff.[72] Member states and UN headquarters should also fill gaps in expertise in JMACs, JOCs, and military intelligence branches, including in areas such as information and data analysis, network analysis, open-source intelligence, monitoring and analysis of mis- and disinformation and hate speech, geospatial analysis, and data management.

The chief of staff plays a critical role working with all units to strengthen data governance and promote the use of data as a mission-wide asset. The chief of staff should ensure that this issue is not relegated to JMAC, JOC, or information and communication officials. UN headquarters should also seek to appoint chiefs of staff with the necessary skills and commitment for effective information management. In general, job profiles for employment in UN peace operations should include information- and data-management expertise.

Strengthen the policy framework for the effective and responsible use of data: While the UN has produced a policy framework for peacekeeping-intelligence, this covers only a fraction of the data needed for mandate implementation. There is no comparable guidance on data that missions handle outside of the peacekeeping-intelligence cycle or that is not fed into Sage or Unite Aware, such as notes from intercommunal dialogues kept by civil affairs sections or perception surveys by strategic communications units. The UN should develop policy, guidance, and training materials for all personnel who work with data to reinforce the message that its responsible management and use is a cross-mission responsibility. A comprehensive policy framework should guide the acquisition, dissemination, use, and destruction of data, specifying accountability mechanisms for its improper handling.[73] Those developing this policy framework could draw on discussions in the online community of practice for data practitioners in peacekeeping operations and special political missions, which was in the process of being established in the summer of 2023.[74]

Provide adequate and predictable funding for data acquisition, analysis, and use: Many recent innovations have relied on bilateral member-state contributions, such as the Indian government's support for the Unite Aware rollout or the Norwegian government's extrabudgetary funding for posts on information management. However, to ensure that data acquisition, management, and analysis are adequately financed with a strategic and long-term vision, greater collective commitment from member states is needed, including sustained financial support. It is therefore crucial that initiatives to support data-related innovations are not concentrated solely on missions that have been of special interest to a particular group of member states (such as MINUSMA).

Enhance internal and external communication about the ways in which UN peace operations gather and use data: In order for new technologies to be accepted and employed effectively, their users and beneficiaries should understand the risks, limitations, and associated opportunities. UN peace operations should inform the population in their area of deployment about how they acquire, store, and use data and how it can help enhance mandate implementation. Internally, operations should do the same for their personnel with a view to reassuring colleagues that information can be

72 One of the barriers to attracting data specialists to work in UN peace operations is the way in which entrance exams for various programs, such as the Young Professionals Programme, are structured. Designed with political science and law graduates in mind, such exams may be perceived as prohibitively difficult for computer science graduates and others with data expertise.

73 Regulating how long data is kept, where, and what options individuals and entities have for withdrawing or modifying it is an essential but overlooked aspect of information security and privacy protection.

74 Interview with UN official, July 2023. Online communities of practice have been found to be useful tools for facilitating exchanges of best practices and horizontal learning on emerging issues in peace operations, such as quick-impact projects. UN General Assembly, *Report of the Office of Internal Oversight Services on the Review of Military Involvement in Civil Assistance in Peacekeeping Operations*, UN Doc. A/60/588, December 13, 2005.

shared securely and demonstrating how new technologies can reduce their workload.

Encourage the proactive use of data in strategic decision making: Data should inform decision making not only at the operational and tactical levels but also at the strategic level. Mission leadership, collaborating closely with the chief of staff, should participate in the development of mission-specific data-governance principles and procedures and help identify formats in which data should be communicated to them. With appropriate safeguards, data should be shared with host-state partners for use in predictive analysis and joint planning. The UN should encourage partnerships with research institutions that could allow it to adopt innovative tools for effective data analysis. Finally, data generated with the help of various platforms, such as Unite Aware and CPAS, should be reported to the UN Security Council in compelling visual formats. For their part, member states should request analysis based on data from the Secretariat and peace operations by posing appropriate questions—for example, asking about trends in violence, socioeconomic effects of conflicts, and perceptions of the mission among the local population. A concerted effort by all elements of the UN system is necessary to harness the potential of increased data availability in an effective and responsible manner.

Annex

Table 1. UN policy frameworks on data in peace operations

Secretary-General's Bulletin on Information Sensitivity, Classification and Handling (2007)	The UN regulates access to information on the basis of a classification system that determines how data should be stored, shared, and protected. It also differentiates between nonsensitive and sensitive information. Nonsensitive information includes public information, which is expected to be disseminated, and unclassified information. Sensitive information includes confidential and strictly confidential information, whose unauthorized disclosure may cause damage or grave damage (respectively) to the work of the organization. It also encompasses personal data, which includes any information relating to identified or identifiable individuals, such as name, location, or social identity (such as gender, age, or sexual orientation).[75]
Secretary-General's Strategy on New Technologies (2018)	The strategy underlines the importance of privacy, human rights, ethics, equality and equity, sovereignty, transparency, and accountability in the implementation of new technologies across the UN system.[76]
UN Military Peacekeeping-Intelligence Handbook (2019)	The handbook has a chapter on the security of military peacekeeping-intelligence that covers information classification, information handling, information security principles, and threats to data integrity. The handbook stipulates that peacekeeping-intelligence must be acquired in a non-clandestine manner, which means that peacekeepers cannot use false identities, engage in covert action, or operate in plain clothes if they are members of the military or police component.[77]
Data Strategy of the Secretary-General (2020)	The strategy calls for adequate protection and privacy of personal data, especially when it comes to vulnerable or marginalized populations; discourages data hoarding by teams or individuals to the detriment of the organization as a whole; and identifies seven barriers to the effective and responsible use of data: data savviness; data quality; governance challenges; change management needs; technology gaps and disruptions; data privacy, protection, and ethics; and funding.[78]
Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook (2020)	The handbook stresses that peacekeeping-intelligence activities must respect human rights—in particular, the rights to privacy and freedom of expression—and must be conducted in ways that do not expose any sources to harm.[79]

75 UN Secretariat, *Secretary-General's Bulletin: Information Sensitivity, Classification and Handling,* UN Doc. ST/SGB/2007/6, February 12, 2007.

76 United Nations, "UN Secretary-General's Strategy on New Technologies," September 2018, available at https://www.un.org/en/newtechnologies/ , p. 4.

77 United Nations, "Military Peacekeeping-Intelligence Handbook," April 22, 2019.

78 United Nations, "Data Strategy of the Secretary-General for Action by Everyone, Everywhere," May 2020, available at https://www.un.org/en/content/datastrategy/index.shtml .

79 UN DPO, "Peacekeeping-Intelligence, Surveillance and Reconnaissance Staff Handbook," September 2020, p. 8.

Guidelines on Acquisition of Information from Human Sources for Peacekeeping-Intelligence (2020)	The guidelines stress that acquisition of information from human sources should not be incentivized by remuneration or other material benefits, cannot be acquired from underage individuals, should not come from host-state officials (unless authorized both by the host state and the head of mission), and should avoid engagement with sources with a history of human rights violations without headquarters's consent. Considering the risks inherent in acquiring, processing, and using information from human sources, the guidelines recommend relying on such sources only when other sources are inaccessible or inconclusive. Human sources should be treated with dignity and respect, and a risk assessment should be conducted to ensure the safety of everyone involved. Sources should be assigned an alias, and the document matching names to aliases must be stored on an encrypted hard drive in a secure location on a device not linked to the Internet or intranet.[80]
Strategy for the Digital Transformation of UN Peacekeeping (2021)	The strategy stipulates that peacekeeping operations should observe the UN's confidentiality, classification, and privacy procedures. It outlines the UN's understanding of the concept of "collective data harms," which includes confidentiality breaches, illegal surveillance, mis- and disinformation, and sabotage or disruption of information systems. The strategy also highlights the risks related to ineffective data sharing and data fragmentation across different information management systems in peace operations and the broader UN system.[81]
UN Guidelines on Open-Source Peacekeeping-Intelligence (2022)	The guidelines highlight how the overall UN ethical principles may apply in situations when peace operations personnel acquire data from open sources (for example, online). The general prohibition on clandestine activities means that UN personnel cannot use fake identities on social media. Illegal activities, such as hacking websites, are strictly prohibited. If peace operations personnel need to access the dark web, they must have prior authorization from headquarters, which already monitors the dark web for any threats to UN peacekeepers' safety.[82]
UN Peacekeeping Missions Military Peacekeeping-Intelligence Surveillance Reconnaissance (PKISR) Unit Manual (2022)	The manual stresses that raw data acquired by intelligence, surveillance, and reconnaissance units should only be shared on a "need-to-know" basis to ensure data protection. It also highlights risks related to objectivity and accuracy of data during its acquisition and processing that stem from limitations such as the sensor's capability, the source's credibility, or the evaluator's judgement.[83]

80 UN DPO, "Guidelines: Acquisition of Information from Human Sources for Peacekeeping-Intelligence," September 1, 2020.

81 UN Peacekeeping, "Strategy for the Digital Transformation of UN Peacekeeping," September 17, 2021, available at https://peacekeeping.un.org/en/strategy-digital-transformation-of-un-peacekeeping ; UN OICT, "Sharing United Nations Official Information with External Parties: Guidelines," 2011.

82 UN DPO, "Guidelines: Open-Source Peacekeeping-Intelligence (OPKI)," March 1, 2022.

83 UN DPO, "United Nations Peacekeeping Missions Military Peacekeeping-Intelligence Surveillance Reconnaissance (PKISR) Unit Manual," October 19, 2022, p. 10.

UN Guidelines on Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities (2022)	The guidelines focus on data security in situations where peacekeepers transmit or obtain data from non-mission actors, such as other UN entities, non-UN operations in the host country, and host governments' security forces. The guidelines outline several principles for receiving and transmitting data to non-mission and non-UN entities, such as maintaining a central registry of all peacekeeping-intelligence shared and received, including orally and by other informal means; sharing only sanitized data (following the removal of information that could lead to accidental identification of sources, witnesses, or survivors); and clearly communicating that peace operations do not accept information obtained through extrajudicial means, such as arbitrary detention or torture.[84]
Reinforcement Training Package for UN Peacekeeping-Intelligence, Surveillance and Reconnaissance (2022)	The training package provides several scenario exercises to help peacekeepers understand their legal obligations. The scenarios stress that the following behaviors are illegal: trading surveillance data on political opposition with a repressive host government in return for information that keeps peacekeepers safe, using data provided by a host state's military intelligence agency if that agency uses violence to extract information from detainees, pressuring a wounded fighter to provide information in return for medical treatment, or sharing information with a regional peacekeeping force with a history of firing indiscriminately at populated areas.[85]
UN 2.0: Forward-Thinking Culture and Cutting-Edge Skills for Better United Nations System Impact (2023)	In this policy brief, which is a part of the so-called Quintet of Change reform drive, focusing on data, digital technologies, behavioral science, foresight, and innovation, the UN commits to investing in responsible data management and governance to assist UN officials in accessing and sharing the data they need in ways that prioritize quality, security, privacy, and human rights.[86]

84 UN DPO, "Guidelines: Sharing Peacekeeping-Intelligence with and Receiving Intelligence from Non-UN and Non-Mission UN Entities," December 1, 2022.

85 UN Peacekeeping Resource Hub, "Reinforcement Training Package: UN Peacekeeping-Intelligence, Surveillance and Reconnaissance (PKISR)," available at https://peacekeepingresourcehub.un.org/en/training/rtp/PKISR .

86 United Nations, "UN 2.0: Forward-Thinking Culture and Cutting-Edge Skills for Better United Nations System Impact," September 2023, available at https://www.un.org/two-zero/en , p. 17.

The **INTERNATIONAL PEACE INSTITUTE** (IPI) is an independent, non-profit organization working to strengthen inclusive multilateralism for a more peaceful and sustainable planet. Through its research, convening, and strategic advising, IPI provides innovative recommendations for the United Nations System, member states, regional organizations, civil society, and the private sector. With staff from around the world and a broad range of academic fields, IPI has offices facing United Nations headquarters in New York and an office in Manama.

777 United Nations Plaza, New York, NY 10017-3521, USA
TEL +1-212-687-4300 **FAX** +1-212-983-8246

52-52 Harbour House, Bahrain Financial Harbour
P.O. Box 1467, Manama, Bahrain

www.ipinst.org