Cybersecurity and UN Peace Operations: Evolving Risks and Opportunities

Dirk Druet

MARCH 2024

Dirk Druet is a Non-resident Fellow at IPI and an Adjunct Professor at the Center for International Peace and Security Studies at McGill University.

The author would like to thank Annika Hansen, Mariana Knaupp, Jenna Russo, Albert Trithart, and an anonymous reviewer for their review of this issue brief.

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

The potential cybersecurity vulnerabilities of UN peace operations are growing. Fast-moving changes in the cyber capabilities of state and non-state actors, the changing nature of asymmetric warfare, and the positioning of the UN in relation to global and regional geopolitics are increasingly placing peace operations in the crosshairs of complex cybersecurity threats. Parallel security actors such as the Wagner Group, among others, raise potential new cybersecurity risks. The increased flow of disinformation in conflict environments may be accompanied by new types of cyberattacks targeting peace operations.

Alongside these external trends, internal trends in missions' intelligence, surveillance, and data management technologies also make them more vulnerable to cyber threats. Mission networks are storing new types of highly sensitive data in more centralized, structured systems and formats. While this increasing centralization has some cybersecurity benefits, it also presents a more readily packaged product for those seeking this information and risks exposing sensitive information. Additionally, practices regarding contingent-owned intelligence and surveillance equipment can effectively eliminate the UN's control over how some data is used and handled.

At the same time, there are opportunities for missions to leverage cybersecurity infrastructure to support the implementation of their mandates, including in the areas of mediation and political settlements and the protection of civil society actors. In this context, the UN should consider the following recommendations:

- The Secretariat should develop cross-cutting operational concepts and guidance for cyber threat assessments in peace operations.
- The Secretariat should articulate its understanding of its duty of care for staff privacy and develop operational guidance and expertise for mitigating threats to privacy.
- When facilitating political processes, peace operations should consider whether cybersecurity measures will be equally effective in deterring hacking attempts by all parties to ensure they do not exacerbate "information asymmetries."
- The UN should explore the boundaries around missions evading or obstructing surveillance or intrusion activities by host states to secure their operations.
- The Secretariat should mitigate the volume of data exposed to external systems, including by deploying UN-owned and UN-operated intelligence and surveillance devices when possible.

Introduction

As state-sponsored cyberattacks, digital surveillance, and cybercrime become increasingly ubiquitous features of the international peace and security landscape, the role of the UN in addressing these phenomena has become hotly debated. The most active threads of this debate have considered the application of international law in cyberspace and the UN's responsibilities in managing cyber threats or disputes.[1] Some analysts have proposed the deployment of "digital blue helmets" to monitor and report on malicious activities, acting as trusted forensics investigators or even taking an active role in disrupting malicious cyber actors.[2]

Less public attention has been given to how trends in cybersecurity affect the UN's current peace and security activities, especially peace operations. While multiple high-profile incidents over the past two decades have highlighted serious vulnerabilities in UN networks, there has been little systematic analysis in the public sphere of how these vulnerabilities impact operations in the field as they are mandated and deployed today. Moreover, comparatively little consideration has been given to how cybersecurity tools and practices could enhance the ability of peace operations to deliver their mandates, despite the emergence of good practices across the system.

> Mission networks are storing new, highly sensitive, and heavily centralized types of data.

Fast-moving trends in the cyber capabilities of state and non-state actors, the changing nature of asymmetric warfare, and the positioning of the UN in relation to global and regional geopolitics are increasingly placing peace operations in the crosshairs of complex cybersecurity threats. In parallel, the deployment of more sophisticated tools for collecting and managing information and intelligence in some peace operations means that mission networks are storing new, highly sensitive, and heavily centralized types of data. In this context, the potential risks associated with cybersecurity vulnerabilities are increasingly consequential.

A growing array of offices within the UN Secretariat is increasingly seized of these challenges, including those responsible for handling information and communication technologies (ICT) in the field, developing intelligence capabilities, and facilitating the digital transformation of peacekeeping. As these efforts advance, peace operations policymakers urgently require a better understanding of the cybersecurity threats facing peace operations and the legal, ethical, political, and operational implications of the Secretariat's ongoing activities to expand missions' cybersecurity capabilities. Building on a previous IPI issue brief on the responsible management and use of data, this paper endeavors to provide an overview of the cyber threats facing peace operations and opportunities to leverage cybersecurity tools for mandate implementation.[3] It also documents the operational and policy challenges that have arisen and the Secretariat's efforts to address them.

For the purposes of analyzing cyber threats in relation to UN peace operations, this issue brief defines cybersecurity as "a collection of tools and measures to protect systems, networks and data from digital attack."[4] The paper draws on document analysis and confidential interviews with UN officials who work in peace operations and at UN headquarters.[5] It should be noted that the paper does not attempt to assess or recommend technical ICT tools and policies for cybersecurity, focusing instead on the strategic positioning of peace operations within the changing world of cybersecurity

1 International Committee of the Red Cross (ICRC), "International Humanitarian Law and Cyber Operations during Armed Conflicts," November 2019.

2 See, for example: Michale Robinson et al., "Developing Cyber Peacekeeping: Observation, Monitoring and Reporting," *Government Information Quarterly* 36, no. 2 (2019).

3 See: Kseniya Oksamytna, "Responsible Management and Use of Data in UN Peace Operations," International Peace Institute, October 2023.

4 In its entirety, the International Telecommunications Union defines "cybersecurity" as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment." See: International Telecommunications Union, Overview of Cybersecurity, UN doc. X.1205, April 18, 2008.

5 Whereas cybersecurity is heavily concerned with the protection of data, trends in the management and use of data by UN peace operations and the risks they face are a paramount concern for the UN's cybersecurity policy. In short, cybersecurity should enable the mission's effective, responsible, and ethical management and use of data. See: Oksamytna, "Responsible Management and Use of Data in UN Peace Operations."

threats and opportunities.

The first section of the paper situates the issue of cybersecurity in peace operations within the broader context of challenges the UN system has faced in protecting its networks from intrusion and discusses the ways in which UN peace operations present a unique case within the UN system. Second, the paper summarizes recent trends in the use of new technologies within peace operations and how they shift the threat profile of the missions in which they are deployed. The third section discusses the impact of external trends, both technological and political, on the cybersecurity risks currently or potentially faced by missions. Fourth, the paper explores how missions' tools and expertise to secure themselves from cyber threats could also contribute to the implementation of mandated tasks such as the protection of civilians. In light of these challenges and opportunities, the final section identifies current or emerging policy questions and provides some initial recommendations on how they could be resolved.

The Longstanding Problem of Cyber Intrusion at the UN and the Unique Risk Profile of Peace Operations

Over the last two decades, multiple high-profile incidents have highlighted serious vulnerabilities in the UN system's ICT infrastructure. The release of documents from the US National Security Agency (NSA) by whistleblower Edward Snowden in 2013 revealed that the NSA systematically gathered signals intelligence both on the Secretariat itself, including through its internal video conferencing service, and on the permanent missions of other UN member states. In the process, the NSA reportedly found that the government of China was doing the same thing.[6]

In early 2013, the General Assembly tasked the secretary-general with developing a system-wide ICT strategy and reporting on efforts to improve information security. The resulting document, released after the Snowden revelations and amid ongoing information security threats, can be considered the UN's first comprehensive cybersecurity strategy. Actions taken under the strategy included the expansion of intrusion-detection services to cover offices away from headquarters, including data centers in Valencia and Brindisi; upgraded firewall infrastructure; and a series of staff education initiatives on what the General Assembly termed "cyber hygiene" due to the relatively low level of cybersecurity awareness among UN staff.[7]

Despite these efforts, the UN has remained vulnerable to cyberattacks. Notable incidents in recent years have included the 2016 revelations that hackers had infiltrated the networks of the International Civil Aviation Authority to plant malware on the systems of member states that interacted with the agency.[8] In 2019, UN offices in Geneva and Vienna, including the Office of the High Commissioner for Human Rights (OHCHR), were hit by a cyberattack targeting their Microsoft SharePoint–based file-management system. In both cases, the UN was criticized for failing to adequately report the attacks, both externally and to its staff.[9] In 2021, it was reported that the UN was fending off a protracted breach of its networks at headquarters in New York and that cybersecurity firms had found evidence of criminals claiming to have access to UN software.[10] In an ongoing sense, a multilateral organization like the UN, which lacks a system of detailed background checks or security clearance management, will always be at heightened risk of "insider threats" posed by staff who knowingly endanger the organization's cybersecurity.[11]

As cyber threats have evolved, the UN's cybersecurity measures have become better tailored to the risk profiles of different types of activities and entities. This includes peace operations, whose risk

6 David Fiddler, ed., *The Snowden Reader* (Bloomington, IN: Indiana University Press, 2013).

7 UN General Assembly, *Progress on the Implementation of Recommendations Related to Strengthening Information and Systems Security across the Secretariat: Report of the Secretary-General,* UN Doc. A/68/552, October 25, 2013.

8 Debra Arbec, "Montreal-Based UN Aviation Agency Tried to Cover Up 2016 Cyberattack, Documents Show," CBC, February 27, 2019.

9 Michelle Nichols, "U.N. Says Offices in Geneva, Vienna Targeted by 'Well-Resourced' Cyber Attack Last Year," Reuters, January 29, 2020.

10 Sean Lyngaas and Richard Roth, "United Nations Confirms Hackers Breached its Systems Earlier this Year," CNN, September 9, 2021.

11 See, for example: United Nations, *Cybersecurity in the United Nations System Organization: Report of the Joint Inspection Unit*, UN Doc. JIU/REP/2021/3, March 2021.

profile is unique among UN actors for legal, operational, and political reasons. Legally, the authorization of peace operations by the Security Council—especially peace operations authorized under Chapter VII of the UN Charter—equips them with distinct permissions and capabilities that impact their risk profile. Peacekeeping missions authorized to use "all means necessary" in situations of violent conflict are arguably justified in gathering more sensitive data on individuals and entities within the operating environment, including through intrusive means. Moreover, the mandated tasks of many missions (for example, in the areas of human rights; political affairs; and disarmament, demobilization, and reintegration) expose them to information that may be of significant interest to the host state, neighboring militaries, and global powers.

In this context, peace operations arguably have a strong justification to employ operational security measures that are more robust and perhaps more expensive than what other UN entities might use. For example, secure radio systems, end-to-end secure physical network infrastructure, and intrusion countermeasures may be necessary to ensure that hostile actors do not learn the maneuvers of troops. When they consent to the deployment of a peacekeeping operation in their territory, host states agree in principle to some level of internal secrecy. Status of mission and status of forces agreements concluded with the host government upon the authorization of a mission generally include provisions allowing for confidential communications within the mission, between the mission and UN headquarters, and even between the mission and external actors such as the International Criminal Court.[12] These provisions at least theoretically provide a degree of recourse for some types of cyber intrusion, especially from the host state, and provide a strong basis for the use of and expenditure on robust operational security measures.

At the same time, the legal status of peace operations under international humanitarian law (IHL) may increase their vulnerability to cyber intrusion. While the precise legal status of peace operations is contested, it is generally agreed (including by the UN) that peacekeepers are at least subject to IHL when engaged in offensive operations, as has been the case with the Force Intervention Brigade in the mission in the Democratic Republic of the Congo (MONUSCO) and during some operations by the mission in Mali (MINUSMA).[13] For peacekeepers subject to IHL, rules on the conduct of war likely allow belligerents to covertly and intrusively seek access to intelligence about their plans and intentions. This does not constrain missions' efforts to thwart these intrusions, but it may limit their capacity to hold belligerents accountable.

> A multilateral organization like the UN will always be at heightened risk of "insider threats" posed by staff who knowingly endanger the organization's cybersecurity.

The 2021 Strategy for the Digital Transformation of UN Peacekeeping broadly acknowledges the unique risk profile of peace operations and that the sensitive information peace operations gather under Security Council mandates raises complex operational challenges and ethical concerns. The strategy foresees several lines of action to address these risks, including the integration of cyber threat analysis into peacekeeping-intelligence activities; improved data governance regimes; and specific protocols to address emerging vulnerabilities resulting from, for example, the use of artificial intelligence (AI) and machine-learning technologies.[14] As the Secretariat implements the strategy, these efforts are continually challenged to adapt to new cybersecurity vulnerabilities. Some of these vulnerabilities emerge from the increased use of digital technologies by peace operations themselves, while others result from the evolving positioning of peace operations within the international peace and security and geopolitical landscapes.

12 Scott Sheeran et al., "UN Peacekeeping and the Model Status of Forces Agreement," University of Essex, August 2010.

13 For an overview of the debates around the legal status of UN peacekeepers, see: Dieter Fleck, "The Legal Status of Personnel Involved in United Nations Peace Operations," *International Review of the Red Cross* 95, no. 891/892 (August 2015); Antonio Garcia, "United Nations Peacekeeping Offensive Operations: Theory and Doctrine," Small Wars Journal, September 28, 2017.

14 UN Department of Peace Operations (DPO), "Strategy for the Digital Transformation of UN Peacekeeping," August 2021.

Internal Trends in Intelligence, Surveillance, and Data Management Technologies

In addition to the ongoing and apparently intensifying challenges of network intrusion faced by the UN, developments in the capabilities that peace operations deploy have exposed them to new vulnerabilities. This is particularly true for intelligence- and surveillance-related technologies and the systems used to store the data and analysis they generate. This section discusses how the introduction of these technologies has impacted the cyber risk profile of peace operations.

While peace operations have always gathered intelligence and deployed surveillance and reconnaissance tools, the introduction of more sophisticated technologies and practices has raised many new challenges for secure data management. As mandates have become more robust and security environments more dangerous, the types of data gathered by peace operations have become more sensitive, and the potential value to hostile actors and potential harm caused by the loss of this data have increased. In 2008, the UN deployed its first large unmanned aerial surveillance drone in Chad, and since then, drones have become standard tools in many peacekeeping operations. Other surveillance and reconnaissance tools have been deployed to generate weapons intelligence, such as systems to detect the origins of improvised explosive devices; signals intelligence, such as the use of mobile phone interception devices by MONUSCO's Force Intervention Brigade; and pattern of life analysis entailing the gathering of large amounts of data to understand the activities and habits of persons or populations. Renewed information security concerns have also arisen over longstanding, lower-tech practices like the gathering of information from human sources when this information is fed into the same systems.[15]

The types of data gathered by peace operations have become more sensitive, and the potential value to hostile actors and potential harm caused by the loss of this data have increased.

Centralized Data Management and Analysis

A visitor to the joint mission analysis center of a peacekeeping operation in the early 2000s might well have come across a hodgepodge of security incident spreadsheets, notes of interviews, and analytical products, some stored on unstructured "shared folders" on mission servers and others on individual machines. This data would in turn rely on reporting from a variety of other sections with a similar array of data management regimes.

Over the last fifteen years, the UN Department of Peace Operations (DPO) has undertaken intensive efforts to structure and centralize information gathered for the purposes of trend analysis and decision-making support. Initially, these efforts were focused primarily on event data (records of incidents such as armed group attacks, military operations, etc.) in a database known as Sage and, for some specialized teams, Microsoft's iBase. More recently, this dataset has been incorporated into Unite Aware, a system for collating and displaying a wide variety of substantive, operational, and administrative datasets.

While the centralization and structuring of data has the obvious cybersecurity benefit of removing sensitive information from individuals' computers and shared folders with few access rights, it also presents a much more readily packaged product for those seeking such information if they are successful in accessing it.

The Digitization and Sharing of Partner, Witness, and Victim Information across Mission Offices

The centralization of data management across peace operations also risks exposing sensitive information gathered through relationships of trust, including the personal identifying information of UN partners, witnesses, or victims of

15 For an overview of the policy and political debates associated with these trends, see: Sarah-Myriam Martin-Brûlé, "Finding the UN Way on Peacekeeping-Intelligence," International Peace Institute, August 2020; Alexandra Novosseloff and Olga Abilova, "Demystifying Intelligence in UN Peace Operations," International Peace Institute, July 2016.

violence. Information of this type is gathered with the informed consent of the subject and often on the basis of a person-to-person or person-to-office relationship.

While efforts to strengthen integration across mission components have encouraged the sharing of information, actual data management and cyber hygiene practices vary across different parts of missions. For example, members of an investigations team in an OHCHR–mission joint human rights office receive some training on information security in the handling of highly sensitive data. This may include training in measures to reduce their exposure to sophisticated cyberattacks, such as the remote installation of software like the Pegasus spyware program, sold by the Israeli company NSO Group to governments around the world. The same cannot be said for other mission offices. A 2021 review of cybersecurity measures by the UN's Joint Inspection Unit recommended significantly expanding "role-based cybersecurity training," targeting personnel "with sensitive missions or… field-deployed staff facing certain location or infrastructure-specific risks."[16]

Such risks are particularly important in many peace operations settings. As OHCHR has reported, many jurisdictions have failed to instate guardrails against hacking operations.[17] Moreover, human rights reporting by peace operations—which in many cases may implicate host states in violations—often leads to tense relations between missions and host governments, placing this information at particular risk. While OHCHR maintains a stand-alone database that mitigates this risk to some degree, information gathered across the mission that is politically sensitive or related to child protection issues or cases of conflict-related sexual violence may not enjoy the same protections.

Contingent-Owned Intelligence and Surveillance Equipment

Some of the intelligence and surveillance technologies used in peace operations are provided and operated as contingent-owned equipment (i.e., they are part of the equipment deployed with a military or police unit provided by a UN member state to a peace operation).[18] Examples include forensic equipment operated by specialized police units and drones operated by intelligence, surveillance, and reconnaissance (ISR) companies in MINUSMA, as well as international mobile subscriber identity (IMSI) catcher devices operated by a signals intelligence unit in MONUSCO's Force Intervention Brigade.

All personnel and equipment deployed to a peace operation are required to operate under UN rules and regulations. Nonetheless, many of these devices are covered by national laws, regulations, and processes for maintaining operational security that constrain the types of data that can be shared with the mission and rules for the storage and retention of that data. Moreover, the operational model used for many of these tools involves sending data back to national capitals for processing—a practice known as "reach-back"—which clashes with UN rules on the ownership of information gathered by peacekeeping operations and disrupts the chain of custody of this information. While national operational security systems may be robust, these rules and practices place some forms of data gathered by peacekeepers outside of the visibility and coverage of UN cybersecurity systems, effectively eliminating the UN's control over how the data is used and handled.

External Trends in Cyber Threats and Their Implications for Peace Operations

As the UN's internal strategies shift peace operations' cyber risk profiles, trends in the "hybridization" of warfare continue to introduce (or often simply exacerbate) cybersecurity threats to peace operations. This section discusses trends in the cyber activities of other actors operating in mission

16 UN Doc. JIU/REP/2021/3.

17 UN Human Rights Council, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, UN Doc. A/HRC/51/17, August 4, 2022.

18 For a detailed discussion of the operational modalities for the use of information-gathering surveillance equipment in peace operations, see: Dirk Druet, "Enhancing the Use of Digital Technology for Integrated Situational Awareness and Peacekeeping-Intelligence," April 2021.

environments and the ways in which those activities impact or potentially impact peace operations.

Parallel Security Actors

Amid the ongoing tectonic shifts in global geopolitics, UN peace operations have found themselves targeted in new ways by security actors in their operational spaces. Most notably, the arrival of Russia's Wagner Group in the Central African Republic (CAR), Mali, Libya, and Sudan has created new risks and challenges for safety and security and effective mandate implementation.[19] Where deployed in peacekeeping environments, the Wagner Group has cast itself as an alternative to the UN, both in defeating insurgent armed groups and as a broader security and political partner to host governments. Wagner forces, often acting jointly with national security services, have impeded missions' ability to protect civilians and investigate human rights abuses, obstructed UN flights, and threatened UN national staff.[20]

In addition to their role in spreading disinformation (discussed below), the proximity of actors like the Wagner Group to peacekeepers raises a variety of potential new cybersecurity risks. These risks are particularly acute where these groups and their political backers have cast themselves in an adversarial relationship with the mission. At a tactical level, missions now need to be more concerned about the security of their communications, including within and among uniformed units using nationally supplied communications equipment. More generally, the operational security measures taken by parallel security actors could include the intrusive surveillance of surrounding areas, posing operational security and privacy risks for units and mission personnel nearby. (This is a risk inherent to all parallel forces operating alongside peace operations.) Furthermore, the deterioration in mission–host state relations, which is correlated with several host states' stronger bilateral ties with Russia, could increase host states' willingness to intrude into UN networks.

> Amid the ongoing shifts in global geopolitics, peace operations have been targeted in new ways by security actors in their operational spaces.

Disinformation, Privacy, and Safety and Security

In this political context, the increased flow of disinformation in conflict environments may incentivize new types of cyberattacks targeting peace operations. As political actors of all types, including politicians and armed groups, increasingly turn to social media to undermine missions' credibility and legitimacy, the threat of surveillance and personalized cyberattacks appears to be growing. Malicious actors could, for example, mine mission networks for embarrassing information.[21] Hackers could take control of mission communications systems, including social media accounts, email systems, or radio broadcast systems, to impersonate the mission. Alternatively, they could plant any number of "false intelligence" scenarios causing the mission to act erroneously, potentially with fatal consequences.[22]

These trends also pose novel threats at the individual level. Mission personnel, including mission leadership, could become the targets of hacking attempts intended to embarrass or undermine them.[23] Additionally, the rapidly expanding capabilities of generative AI could provide new ways for manipulating and deploying information to target individuals, units, or missions as a whole. These threats present a range of traditional safety and security challenges, such as the risk of targeted violence against individuals as a result of information shared online. They also present new, serious threats not currently covered by the UN's Security Management System. For UN personnel and those they communicate with, these include violations of privacy, personal consequences from having private information released, and violations of bodily autonomy through the spread of fake images or videos.

19 See, for example: Christoph Matschie and Annika S. Hansen, "Russia's Double-Bluff: The Wagner Group and UN Peace Operations," ZIF Centre for International Peace Operations, July 2023.

20 Dirk Druet, "Wagner Group Poses Fundamental Challenges for the Protection of Civilians by UN Peace Operations," Global Observatory, March 20, 2023.

21 Eleonore Pauwels, "The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI," United Nations University Centre for Policy Research, 2019.

22 Albert Trithart, "Disinformation against UN Peacekeeping Operations," International Peace Institute, November 2022.

23 Chloe FitzPatrick, "Cyber Peace: The Risks of IT Deployed to UN Peacekeeping Missions" (PhD dissertation, University of Queensland, 2021).

Opportunities to Harness Cybersecurity for Mandate Implementation

While missions work to strengthen their own cybersecurity, there are also opportunities for them to leverage that infrastructure (either directly or through the provision of advice and expertise) to support the implementation of their mandates. This section highlights ways in which cybersecurity can positively impact mandate implementation, often drawing on existing practices.

Mediation and Political Settlements

The core objective of most peace operations is to achieve or assist in the implementation of agreements negotiated among the parties to the conflict. Mediation, political facilitation, and the accompaniment of peace processes are therefore important functions for many mission personnel, especially senior leadership. For the UN to play an effective role as mediator, all parties involved must consent to its role. Since all parties to such negotiations have an interest in gaining knowledge of their counterparts' priorities and red lines, as the UN's Guidance for Effective Mediation states, "the integrity of the mediation process, security and confidentiality are important elements in cultivating the consent of the parties."[24] Similarly, UN mediators themselves have an interest in maintaining confidentiality to ensure that their credibility is not undermined and their strategies are not manipulated by the parties.[25]

The "Digital Mediation Toolkit" of the Department of Political and Peacebuilding Affairs (DPPA) acknowledges that "most mediators work under the assumption that their communications are constantly monitored and thus increasingly rely on encrypted email and messaging applications."[26] It therefore advises that "digital security and safety" tools and processes, including the use of encrypted devices and software to guard against the interception of communications and other data, be integrated into all mediation efforts. However, when considering appropriate cybersecurity measures, UN mediators need to account for potential asymmetries in the cyber intrusion capabilities of parties to the negotiation. If these measures are effective in thwarting intrusions by only some of the parties, "this risks further aggravating existing asymmetries between the parties in certain conflicts."[27]

Protection

In an era in which pervasive, AI-driven surveillance places human rights defenders, journalists, and other critical civil society actors under intense pressure, activities to help these individuals and groups operate securely could become an important part of missions' protection work. While any such activities could bring missions into conflict with host-state authorities, they would also arguably be in line with missions' broader efforts to leverage their political influence to protect civil society actors that might otherwise suffer repression.

> Maintaining secure and independent information and communications infrastructure in mission areas could help maintain the continuity of protection activities.

Similarly, maintaining secure and independent information and communications infrastructure in mission areas could help maintain the continuity of protection activities when state or non-state actors make it difficult for national human rights and protection actors to share information or communicate using national ICT infrastructure. This is particularly important when states impose national or area-based Internet and communications blackouts. In Mali, for example, MINUSMA's satellite-based Internet infrastructure allowed it to collect, analyze, and report on violence against protesters despite Internet shutdowns in the lead-up to the announcement of the results of national elections

24 United Nations, "Guidance for Effective Mediation," September 2012, p. 8.

25 UN Department of Political Affairs (DPA), "Mediation Start-Up Guidelines," 2011, p. 11.

26 UN DPPA, "Digital Technologies and Mediation," March 2019, available at https://peacemaker.un.org/digitaltoolkit .

27 Ibid.

in 2021.[28] More recently—and looking beyond UN peace operations—the cross-border movements and multinational footprint of the United Nations Relief and Works Agency (UNRWA) allowed it to continue monitoring and reporting on civilian deaths caused by the Israeli military's invasion of Gaza.[29] UNRWA was able to conduct this monitoring despite the complete shutdown of Internet and mobile phone services on October 20–21, 2023, which made it virtually impossible for Gaza-based protection actors and journalists to share information.[30]

Conclusion and Recommendations

The trends and opportunities discussed above point to the following important and often novel policy considerations for peace operations as they seek to operate in an increasingly fraught political and cybersecurity environment.

- **Integrated cybersecurity threat analysis:** Currently, responsibility for cybersecurity threat assessment is a primarily technical exercise led by the Office of Information and Communication Technology at headquarters and field technology services in missions. To confront the increasing use of cyberattacks in peace operations environments, the UN requires a more integrated approach focused on harnessing partnerships for sharing threat intelligence, building internal cybersecurity capabilities, and increasing technological support to missions. The Secretariat should develop cross-cutting operational concepts and guidance for integrated support and substantive cyber threat assessments that include the UN Department for Safety and Security (UNDSS), the Department of Operational Support (DOS), and DPO, especially joint mission analysis centers, strategic communications and public information offices, and information integrity units.
- **Privacy as a factor of safety and security:** Loss of privacy is not currently considered a safety and security threat under the UNDSS security management system. Yet the loss of privacy as a result of a malicious act can have real and permanent consequences for the well-being and livelihood of personnel and may also beget other threats. Responsibility for protecting the privacy of staff and related personnel in the performance of their duties (as opposed to, for example, medical or other personal data held by the mission) is ambiguous, if indeed the UN believes such a responsibility exists. The Secretariat, including the new UN Privacy Office, should articulate its understanding of its duty of care for staff privacy and develop operational guidance and expertise for mitigating threats to privacy.
- **Intrusion asymmetry in political processes:** As part of their efforts to mediate and support the implementation of political settlements, UN peace operations with cybersecurity measures in place should consider whether these measures will be equally effective in deterring hacking attempts by all parties. If one party is able to access secure information that another party cannot, this may lead to information asymmetry in negotiations that could undermine confidence in the process or in the UN as a mediator. Under such conditions, it may be preferable to adopt an approach of sharing as much information as possible or recording as little as possible in digital form.
- **The boundaries of evasion:** Peace operations have a strong legal basis for maintaining secure communications within the mission and, conceivably, with its interlocutors. In environments in which the host state or a parallel security presence is considered a serious threat to cybersecurity, missions may need to directly evade or obstruct surveillance and intrusion activities to secure their communications. The degree to which these activities are legally justifiable, operationally necessary, and politically viable needs to be explored, especially in the case of communications with non-mission personnel.

28 Jane Esberg and Christoph Mikulaschek, "Digital Technologies, Peace and Security: Challenges and Opportunities for United Nations Peace Operations (Third Draft)," August 2021.

29 UNRWA, "UNRWA Situation Report #11 on the Situation on the Gaza Strip and the West Bank, Including East Jerusalem," October 22, 2023.

30 Abu Bakr Bashir et al., "34 Hours of Fear: The Blackout that Cut Gaza Off from the World," *New York Times*, October 29, 2023.

- **Ownership and custody of information as it relates to cybersecurity:** When deploying surveillance and intelligence technology and practices, clashes remain between national operational security imperatives and principles of UN data ownership. While it will be difficult to fully reconcile these clashes, the Secretariat should take steps to mitigate the volume of data exposed to cyber threats. These could include deploying, wherever possible, intelligence and surveillance devices owned and operated by UN personnel and, where contingent-owned devices are in use, including measures in legal agreements with troop- and police-contributing countries to ensure the protection and limit the use and sharing of data gathered under Security Council mandates. Even in cases where the UN procures equipment directly, it is crucial to ensure security in the supply chain, particularly in situations where the suppliers of sensitive technologies are closely linked with member states' national defense industries.

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