zif Center for International Peace Operations

100 Voices on Technology & Peace Operations

Exploring the impact of digital technology on conflict dynamics and peace operations

Unpacking Challenges and Threats in the Secretary-General's Strategy on the Digital Transformation of UN Peacekeeping

28 September 2021 | Dr. Camino Kavanagh

On 18 August 2021, the United Nations Secretary-General outlined to the Security Council his Strategy for the Digital Transformation of UN Peacekeeping.[1] Echoing what experts within and outside the UN have been warning of for the past few years, and building on his earlier New Technologies and Data strategies as well as the Action for Peacekeeping initiative and priorities, the Secretary-General stressed that digital technologies are changing the character of conflict, with civilians and peacekeepers increasingly at risk of their misuse and abuse.[2] To address these and other associated challenges he noted that the UN will need to "fully embrace the digital world" and "improve the UN's agility, anticipation and responsiveness to conflicts …", which will require both "a shift in culture and systemic change".[3] For anyone familiar with UN peacekeeping, this is undoubtedly a big ask for the organization in terms of resources, capacities, capabilities and enabling infrastructure. And it is a big ask for UN member states, host countries and T/PCCs, particularly in today's geopolitical climate, where resources can be limited and digital technologies (and competing views on how they are governed) move ever-closer to states' strategic interests. It is, nonetheless, an issue that requires urgent attention.

The Strategy itself highlights some of the challenges that UN peacekeeping is encountering, placing emphasis on the need for greater awareness and analytical capacities and capabilities to better understand how technology-enabled changes in the conflict environment affect mandate implementation, peacekeepers and peacekeeping infrastructure. The more malign uses of digital technologies in peacekeeping contexts that the Strategy highlights include "disinformation, misinformation and incitement to violence through hate speech, (…) surveillance, control and intelligence gathering," as well as "recruitment into armed groups, and (…) cyberattacks".[4] As likely discussed in the consultations that shaped the Strategy, the intent of these uses is wide-ranging, and their effect can be both immediate and long-lasting. They are rarely isolated from other conventional political or military tactics and can be deployed by parties both in and beyond the country within which the peacekeeping mission is operating. Other challenges highlighted in the Strategy relate to the introduction of extant and emerging technologies into peacekeeping environments in support of

mission implementation, how these and the data they collect, store and process are managed; how cyber resilience, information security and cyber hygiene practices in mission environments can be improved; and how more responsible use of digital technologies writ large in these contexts must be ensured.

But let's take a step back. Placing some of the aforementioned digital-technology-related threats and challenges in context can help the Strategy's multiple target audiences understand the complexities at hand and what it will take to respond to them. Take, for instance, the following semi-fictional scenarios:

SCENARIO 1

Issandrak is a political affairs officer supporting the UN peace operation's discreet efforts to engage with the one armed group that has remained outside the formal peace process and that has thus far refused to sign the lasting peace agreement. He has spent the weekend preparing a document for the mission's top leadership ahead of the first encounter in over a year with the leader of the group. The document is highly sensitive as it includes details of who will participate in the meeting, their personal details, where the meeting will take place and the issues that will be addressed in the meeting. Issandrak has been using an encrypted communications app to engage with his contact in the group so was surprised when an email from the same person popped up on his desktop marked urgent. According to the email, there was a last-minute change to the list of persons participating in the meeting, and a new list was attached for Issandrak's attention. He clicks on the document. His screen freezes momentarily but then flickers back into action. He breaks into a cold sweat as he recalls his latest OICT Safety in the Field training, realising that he has likely fallen victim to a phishing attack. He quickly tries to turn off his computer and disconnect it from the mission network. Given the focus of his work, it is likely the sensitive documents he handles were the objective of the intrusion, which he knows may put the talk and the members of the rebel group at risk. Issandrak calls his OICT colleagues for support hoping they can immediately assess the extent to which his computer and data have been compromised so he can brief his boss accordingly.

SCENARIO 2

A UN Mission team comprised of national and international communications and civil affairs officers is about to set off on a 2.5-hour journey to a small town north of the regional headquarters to conduct a joint capacity building effort with local journalists, radio producers and bloggers on approaches to dealing with fake news and targeted disinformation. They are accompanied by the usual military escort. Upon departure, a member of the team notes that a video depicting the SRSG lambasting the country's main opposition party for illicitly funding its activities has appeared on social media. By the time the UN team arrives at its destination, the video has gone viral and is eliciting strong reactions. The town where the capacity building effort is set to take place is a stronghold of the opposition party and the UN mission's capacity building partners there are visibly

angry, as is the local population. The UN team has learned that the video was produced using deep fake technology but it is unclear who is responsible for disseminating it. The analysis cell at mission HQ had been warning of escalating narratives on social media targeting the UN operation and the SRSG. Like other peacekeeping operations, this one had been the target of negative social media coverage before, but this time the attacks were virulent, appearing shortly after the SRSG and the broader diplomatic community called on the government to restore connectivity after a series of internet shutdowns in the run up to the elections had affected areas where opposition party supporters reside. This morning's deep fake video has now been circulating for more than four hours. The strategic communications team at HQ has not yet managed to establish contact with the social media platform where the video was posted and the Mission has not yet made a public statement. A stone suddenly comes crashing through the front window of the UN team's vehicle…

SCENARIO 3

After a fitful night's sleep, the UN SRSG prepares for her meeting with the President. This is the third meeting during which mission capabilities to protect civilians will be discussed in accordance with the resolution establishing the UN peacekeeping operation in the country.[5] The situation in the south of the country is highly complex, as extremist groups are advancing into rural areas with reports of abductions and killings of civilian population increasing. Following months of negotiation with TCCs, the SRSG has finally received a commitment of surveillance drones from 3 member states, two of them members of the Security Council. The expectation is that the drones will bolster situational awareness, providing eyes in the sky for the small military brigade that was just authorised to deploy to that region in support of national counter-terrorism operatives. This is not the first time the UN will use non-lethal aerial surveillance drones in a UN operation. The government is aware of some of the thorny discussions that have taken place regarding ownership of the data that will be collected and stored by the Mission and is keen to advance discussions so that it, too, will secure access to that data. Human rights groups are putting pressure on the Mission to ensure that before drones are authorised, it should anchor a commitment by the government to put in place the necessary legal safeguards to protect the rights, privacy and data of individuals and communities throughout the country, including when peace is restored in the country. For her part, the SRSG wants to advance the deployment of the drones as soon as possible, especially given the growing civilian death toll on the ground, but knows she cannot advance without a commitment by the host government to the aforementioned legal safeguards. She is equally concerned about when the supporting drone infrastructure will arrive and how it will be maintained, and has numerous questions about the expertise required to process the data from the drones so as to enable operations on the ground.

SCENARIO 4

It's a rainy morning in the east of the country. The UN mission Force Commander is in town to attend a ceremony that will commemorate several civilians and UN military and civilian personnel who died in an IED attack against a UN convoy last month. The ceremony, co-hosted by local

officials, had been a solemn event held under tight security conditions. Just as he was preparing to fly back to the capital yesterday evening, the Force Commander received an urgent request from the SRSG to extend his mission to address a brewing crisis: across the eastern region critical information infrastructure has been sabotaged leaving tens of thousands of people without mobile and internet connectivity. Most assessments point to a militia group active in the region as being responsible for the multiple incidents of sabotage. Bad weather conditions and high insecurity in the region have prevented the main telecommunications operator from assessing the damage and re-establishing connectivity. The UN regional office was initially unaffected by the incident since it relies on its own, separate communications network. In fact, it had been serving as a relief communications hub for the local hospital and other emergency and essential public services for the past two days. However, this morning the network is down after suffering an attack in the early hours of the morning. It has proved impossible to establish contact with the Remote Mission Support Unit and localized efforts to restore connectivity are ongoing. An initial assessment points to the same militia group being responsible for the breach, although given the nature of the incident, it is likely they received support from a third party. All UN personnel have been ordered to remain at base and a crisis cell has been established, providing hourly reports to the Force Commander. Meanwhile, the Force Commander is commencing an emergency meeting with the regional governor and regional representative of the main telecommunications company operating in the affected region. He is not yet sure how to respond to a request from the regional governor to deploy UN troops to secure critical information infrastructure across the region. He first needs to assess how quickly (if at all) the telecommunications operator can re-establish mobile and internet connectivity in the affected areas and how it plans to mitigate against such acts of sabotage in the short and long-term. The head of OICT was set to join him at the meeting but she is busy dealing with the UN's own communications crisis. A long day lies ahead…

Elements of these and likely more complex and serious scenarios, are what peacekeepers already face on a daily basis. It is becoming increasingly difficult to silo off one specific issue or challenge from another, and even more so from the broader political and security context within which the technologies are used or misused. The current drive to ensure resilience and strengthen cyber security and cyber hygiene practices to protect mission personnel, data, infrastructure and networks needs to continue and must be prioritised at the highest levels of management. Some operations may need to prioritise strategic communications more than others,[6] but that does not mean that the operation should not equally prioritise anchoring the blended analytical capacity – at HQ and in the field, military and civilian – required to understand how competition and control of critical internet resources plays out in different peacekeeping settings, the growing trend in targeted internet takedowns or sabotage of critical information infrastructure at critical political junctures a case in point. Such analytical capacity will also need to identify if and how cyber and other such capabilities are used by different parties to advance their goals and the potential implications of such uses for mandate implementation, particularly the protection of civilians, and the critical contacts and partnerships that need to be developed to ensure continuity in the event of a major incident or event. Indeed, the consequences and harms of critical humanitarian

or information infrastructure or other such essential services being affected by a cyber attack in a peacekeeping environment would be significant.

Furthermore, UN peacekeeping cannot afford to ignore the normative backdrop against which digital technologies are introduced into peacekeeping environments and the lasting effect on civilians if the appropriate human rights, ethical and privacy safeguards are not considered from the outset. These issues will no doubt be central to peacekeeping mandates, as well as to negotiations on troop, resource and technology contributions and other key issues such as ownership of the data gathered through technology-related contributions. Nor can UN peacekeeping ignore the broader normative debates underway at the Security Council, the General Assembly and elsewhere on ICTs and international security relevant to the responsible behaviour of states in their use of ICTs and the value of some of the recommendations put forth by expert groups in these processes to the prevention and protection mandates of peacekeeping.[7]

The new Strategy and other, on-going work within the Secretariat on a number of still-disconnected fronts provides a basis for addressing most of these eventualities. Needless to say, implementation will be no easy task.

FOOTNOTES

[1] Strategy for the Digital Transformation of Peacekeeping, August 2021. See also, Camino Kavanagh, 2020, 'Digital Technologies and Civil Conflicts: Insights for Peacemakers', EU Institute for Security Studies.
[2] Secretary-General Strategy on New Technologies, September 2018; UN Secretary-General's Strategy on Data Management 2020-2022; Action for Peacekeeping (A4P); Action for Peacekeeping Priorities (A4P+).
[3] Secretary-General's presentation to the Security Council on the Strategy for the Digital Tranformation of UN Peacekeeping. Wednesday, 20 August 2021.
[4] Ibid. Strategy for the Digital Tranformation of UN Peacekeeping, p.5.
[5] See also UNSC resolution 1894 of 2009, which called on the Secretariat to give priority in decisions "about the use of available capacity and resources, including information and intelligence resources, in the implementation of mandates" precisely for the protection of civilians. 'Peacekeeping Intelligence'. United Nations Department of Peace Operations, Ref. 2019.08.
[6] See, for instance, Jake Sherman and Albert Trithart (2021), 'Strategic Communications in UN Peace Operations: From an Afterthought to an Operational Necessity', International Peace Institute.
[7] For the latest consensus reports, accompanying and background documentation stemming from these processes, see: UNODA, https://www.un.org/disarmament/open-ended-working-group/ and https://www.un.org/disarmament/group-of-governmental-experts/. See also, Camino Kavanagh and Paul Cornish, 2020, 'Cyber Operations and Inter-State Competition and Conflict: The Persisting Value of Preventive Diplomacy, pp.14-21, and Sean Kane and Govinda Clayton, 2021, 'Cyber Ceasefires: Incorporating Restraints on Offensive Cyber Operations in Agreements to Stop Armed Conflict, CSS, ETH-Zurich.

100 Voices on Technology & Peace Operations

ABOUT THE AUTHOR

Dr. Camino Kavanagh is a Visiting Senior Fellow at the Department of War Studies, King's College London, a Non-Resident Scholar with the Carnegie Endowment for International Peace, and also works as an independent consultant.