TECHPOPS

Center for
International
Peace Operations

100 Voices on Technology & Peace Operations

Supporting the implementation of mandated tasks through digital technologies

Predict and prevent: overcoming early warning implementation challenges in UN peace operations

23 September 2020 | Allard Duursma & John Karlsrud

Early warning has traditionally hampered many peacekeeping operations. When reflecting upon the UN experience in Rwanda during the 1994 genocide, the Force Commander for the United Nations Mission in Rwanda, Roméo Dallaire, notes: "I had no means of intelligence on Rwanda. [...] We always seemed to be reacting to, rather than anticipating, what was going to happen."

PROGRESS HAS BEEN MADE

However, the UN has made some real progress since the turn of the century when it comes to early warning as an integral part of Protection of Civilians (PoC) mandates. Most early warning tools currently in use in peacekeeping missions still take the form of a qualitative analysis conducted by a group of experts. Examples include MONUSCO's forward-looking Protection of Civilians Risk Assessment Framework, UNAMID's Community Alert Network (CAN), and MINUSCA's Flashpoint Matrix.

ENTER THE DATA AGE

Some of these qualitative early warning tools are very good, but these analyses should be supplemented with a data-driven early warning system to help information analysts and the mission leadership identify threats, as well as promote forward thinking. Such tools are now in reach because peacekeeping operations have implemented a web-based database system that allows mission personnel in the field to log incidents, events and activities. Referred to as the Situational Awareness Geospatial Enterprise (SAGE) event database, this database not only includes incidents pertaining to armed violence, but also includes information on incidents like troop movements, increased tensions, hijackings, abductions, protests, and many more potentially relevant incidents. SAGE data is accessible to all sections/components in a mission, for whom access to incident/

event data is required. For example, in MONUSCO and UNMISS, both uniformed and non-uniformed components contribute to and access shared data from SAGE. In-mission, the Joint Operations Centre (JOC) acts as the facilitator and information-broker within the SAGE information management workflow. By allowing multiple components to share their data in a single central database, under the custodianship of the JOC, SAGE aims to provide a Common Operational Picture to the entire Mission. It also eliminates the traditional wasteful duplication of each component creating its own separate database of essentially the same set of incident data. Missions are also using SAGE to report information and create useful data at the same time, replacing the paper-based Daily Situational Report-format of daily reporting from various components to JOC.

PREDICTIVE PEACEKEEPING IS POSSIBLE

Gathering structured data in SAGE enables mission leadership to identify trends and monitor indicators for early warning. When the identification of trends is augmented with machine learning tools, it enables what we refer to as predictive peacekeeping: "a range of analytic tools and peacekeeping practices that serve to forecast where and when armed violence will take place, combined with changes in peacekeeping leadership decision-making, particularly deployment of peacekeeping staff, based on those forecasts." Predictive peacekeeping enables UN staff in the field to improve anticipating and acting on rather than reacting to unfolding events. The SAGE data can also be combined with other data accessible to UN peacekeeping in the situational awareness platform Unite Aware. The challenge remains coverage of large and partially inaccessible theatres of operation and the alert-response gap, both of which are a function of territory and topography/accessibility. Several missions, including MONUSCO, also use unmanned aerial systems (UAS or drones) to monitor population displacements and movements of armed groups.

CHALLENGES MUST BE TACKLED

However, one cannot just assume that a data-driven early warning system will change everything for the better. The UN, at field and headquarters levels, as well as member states should be vigilant when it comes to mitigating the possible negative side effects of a data-driven early warning system. Five major challenges for the UN to set up a data-driven early warning system stand out. We discuss these challenges below and also suggest some ways to address these challenges as best as possible.

COMPREHENSIVE DATA SHOULD BE SHARED HORIZONTALLY

A first challenge is obtaining comprehensive data for an early warning system. Any data-driven early warning system will obviously have to rely on data. The various sections of a UN peacekeeping operation typically collectively produce a firehose of reports, so one would think drawing on comprehensive set of data should not be a challenge for early warning in the UN. However, data is not always shared horizontally with all relevant parties within peacekeeping missions. The challenge of horizontal information sharing within UN peacekeeping missions is a result of an incentive structure that favours sending information up the chain of command. Because the status of units within the mission partly comes from the quality and amount of information they are able to impart with mission leadership, these units are sometimes inclined not to share their collected information horizontally. A whole-of-a-mission approach towards early warning could help to promote horizontal information-sharing, notably at the level of field offices where data is collected and analyzed. The development of SAGE is a great step forward in this regard, because it integrates data from all units and sections within the mission and removes duplicates. However, SAGE is a platform and does not replace the importance of consolidating data into a structured analytical report. Hence, coordination through field office or HQ level mechanisms remains critical.

DATA MUST BE MANAGED SECURELY

A second challenge relates to securely managing the data used for the early warning tool. There is always a risk that these data fall into the wrong hands. The UN has already become the target of offensive cyber-attacks. Cyber-attacks could aim to retrieve data or even change data to alter the understanding of the reality on the ground. Anyone responsible for the early warning system should therefore decide where the data will be stored, how it will be kept secure, and how long data should be stored. However, data breaches can also come from the inside, making it necessary to decide who in the peacekeeping mission and at the Headquarters in New York has access to the raw data underpinning the early warning output. This means that there is a clear tension between resolving the challenge of data-sharing and working towards a whole-of-a-mission approach on the one hand and secure data storage on the other hand.

MACHINES WILL NOT REPLACE CONTEXTUAL KNOWLEDGE AND ANALYSIS

A third challenge is that the over-reliance on a data-driven early warning tool might come at the expense of contextual knowledge peacekeeping staff responsible for early warning should have within the mission. A significant reduction in face-to-face engagements due to budget cuts and a shift towards the use of data can lead to an erosion of contextual knowledge. There is a limit to the extent to which information can be transferred via situation reports and incident reporting. Any data-driven early warning system should therefore be used in addition to early warning tools such as the Community Alert Network (CAN), which is a network of locally recruited Community Liaison Assistants (CLAs) who work with local security committees collecting information on security threats.

BEWARE OF DATA BLIND SPOTS

Fourth, peacekeeping staff responsible for early warning should be aware of the potential effect of what Larrauri and Kahl refer to as the bias of connectivity. Some groups may be more able to use a given technology than other groups. For instance, phones are used more by young, urban, and relatively wealthy people. This means that any early-warning system that makes use of information collection via phones would be skewed towards those that are connected. To mitigate this, MONUSCO has, for instance, issued sim cards to local security committees and CLAs. Still, in some areas there may be no connectivity at all. Within the context of peacekeeping operations, it is plausible to surmise that the UN is better able to collect information in areas in which peacekeepers are deployed. Accordingly, the use of a data-driven early warning tool is likely to be more accurate in locations proximate to peacekeeping bases. A comparison of UN data and data based on media reports suggest that the UN's data collection in Darfur was relatively less comprehensive in areas in which no peacekeepers were deployed. Hence, one important precautionary measure the UN could take is to not solely rely data generated within the UN system, but also on media reporting and reports issued by CLAs.

FROM PREDICTION TO PREVENTION

Fifth, and lastly, a top-notch data-driven early warning system will have little added value if this system is not translated into more effective early action. Edward C. Luck, the Special Adviser to Assistant Secretary-General Ban Ki Moon, pointed out in this regard that early warning is not an end in itself: "Early warning without early and effective action would only serve to reinforce stereotypes of UN fecklessness, of its penchant for words over deeds." It was noted in an inspection report on the performance of UN missions' operational responses to Protection of Civilians related incidents that the time until the UN reacted to attacks on civilians is on average 2.8 days. A data-driven early warning tool is of little value if there is no effective system in place to translate early warning into early action.

MOVING SLOWLY IN THE RIGHT DIRECTION?

To conclude, the UN will need to find a way to analyse the enormous amount of data it produces every day. Machine learning to detect patterns in these data and produce early warnings holds great promise in this regard. However, the use of new technologies is not without risk. Collected data can fall into the wrong hands. With budget cuts missions have been forced to reduce their footprint in the field, increasing the reliance on technology. New technology also requires new types of specialist expertise to manage data, and better understanding among all staff of how data should be managed, vetted and put to use. Some have expressed concerns about the use of technologies being at the expense of face-to-face engagements, ultimately resulting in peacekeeping efforts that are divorced from realities on the ground.

From a practical point of view, the UN will also have to resolve an uneasy tension between enabling access to these data in order to conduct data-driven early warning analyses on the one hand and the need to prevent any data breaches on the other hand. The UN has made progress in the adoption of new technologies to predict and prevent local violence. To maintain the momentum, it needs to continue to innovate to be able to serve people in need faster, better, and more efficiently.

ABOUT THE AUTHORS

Allard Duursma is a Senior Research at the Center for Security Studies (CSS) at ETH Zurich. His work focuses on mediation, peacekeeping, and early warning. He is a Deputy Editor of the journal of International Peacekeeping.

John Karlsrud is a Research Professor at the Norwegian Institute of International Affairs (NUPI), working on peacekeeping and related issues. He has previously served as Special Assistant to the United Nations Special Representative in Chad. He is also a Deputy Editor at International Peacekeeping.