TECHPOPS

100 Voices on Technology & Peace Operations

Partnering for digital technology innovation

Real-time conflict monitoring using artificial intelligence for peace operations

12 October 2022 | Dr. Dirk Kolb & Philipp Starz

By the start of 2022, there were 5.31 billion unique mobile phone users, 4.95 billion internet users, and 4.62 billion active social media users (Datareportal) - all potential sensors for conflict monitoring, and real-time information sharing through their interconnectedness. In 2021, the United Nations (UN), a host of regional organizations and alliances, and ad hoc coalitions of states carried out 63 multilateral peace operations in 38 countries or territories around the world (SIPRI Multilateral Peace Operations in 2021) , representing millions of potential sensors and resulting in a huge amount of Publicly Available Information (PAI) ready for peace operations analysts to use and evaluate to better understand their area of operations. However, without Artificial Intelligence (AI) and Machine Learning (ML) tools supporting Open-Source Intelligence (OSINT) employed for real-time conflict monitoring it would be impossible to exploit its full potential for peace operations.

OPEN-SOURCE INTELLIGENCE (OSINT) FOR PEACE OPERATIONS

During ongoing peace operations, deviations from normality are of major importance for the correct assessment of any ongoing situational changes, and may considerably impact the protection of one's military personnel and the affected civilian population. Analysts try to find answers to questions every day, e.g. where and when the next deviation or conflict will occur, and what their impact on operations, personnel, and the operational environment are. Unfortunately, it happens all too often that new situations seem to come as a surprise, despite the fact that, quite frequently, pertinent data or information were already available but remained undiscovered. In some cases, human sources (HUMINT) are simply prevented from obtaining or reporting the relevant information due to all kinds of impediments, with OSINT remaining the only workable source of information.

Take the complex and interconnected events that took place at the end of the NATO-led Resolute Support Mission in Afghanistan in August 2021. Retrospectively, sufficient information had, indeed, been available that could have led to the conclusion that the situation would evolve the way it

eventually did. Experts already agree that the consistent evaluation of PAI through OSINT would have contributed to a much better appraisal of the situation.

Research shows that 80 percent of information processed by intelligence and analytical bodies in UN peace operations originates from PAI, making OSINT nowadays a discipline that significantly dominates other intelligence disciplines (Nikolić 2017). The great advantage of OSINT consists in considerably reducing the number of demands for classified intelligence collection by limiting requests for information to those questions only that ostensibly cannot be answered by PAI (Steele 2007). Another benefit of using OSINT is the broader dissemination of intelligence since it can be made available to other stakeholders without having to keep secret the sources or collection methods involved (Cament 2007). However, experts also underline the necessity for peace operations to monitor PAI like social media more systematically (Abilova & Novosseloff 2016).

Social media intelligence (SOCMINT) is a powerful subcategory of OSINT. SOCMINT refers to information emanating exclusively from social media platforms. By tracking and constantly monitoring social media, analysts can gain real-time insights into public opinion even in volatile environments. Nordli and Lindboe (2017) for example pointed out that many major conflict actors in Mali use social media for raising their profile with the public, displaying and maybe showing off their capabilities, and activating their supporters. The monitoring of social media has proved to be useful to gain situational awareness and an in-depth understanding of the sentiments of the population in general and in the different factions in particular (Nordli & Lindboe 2017).

NEED FOR ARTIFICIAL INTELLIGENCE ASSISTANCE SYSTEMS

Conflict prevention has become a field in which UN agencies and conflict mediation teams use data capture technologies and intelligence collection to map and better understand recurrent conflict patterns, and forecast potential crises (Pauwels 2020). But all these solutions have their limitations when it comes to creating the most accurate and comprehensive situational awareness.

While capturing PAI has never been as easy as today, turning that data and information into actionable intelligence for decision-making remains one of the biggest challenges for peace operations nowadays: How can we reduce the amount of PAI to focus our resources on the truly valuable and pertinent information we need for a better understanding of current operational challenges? New technological approaches will allow for more predictive analytics, thus enhancing the early warning potential signaling emerging conflicts and operational risks (Wählisch 2020).

To provide peace operations with relevant situational information in near real-time, instantaneous data and information collection as well as AI-based evaluation are indispensable. To this end, a host of AI-based Natural Language Processing (NLP)/Machine Learning (ML) tools are available or under development, e.g., automatic translation in over 100 languages and dialects, sentiment and predictive analysis, or instant geographical location of events, persons, or means of transport. But peace operations analysts quickly reach their limits here: They normally do not speak 200 languages and

cannot read 100 million articles of PAI per day. For example, during operations in Afghanistan, the intelligence collection, processing, and analysis of text and speech data were considerably hampered by the language inadequacy of the analysts involved. (Rietjens 2022).

Therefore, peace operations need assistance systems capable of relieving the analyst of the hard work by providing already pre-categorized/pre-filtered data and information. Already existing event codebooks like those of GDELT or ACLED are tailored to specific situations, e.g. military conflicts, political crises or disaster warnings:

- Global Database of Events, Language, and Tone (GDELT): The GDELT project collects information from a wide variety of data sources and categorizes it, using the Conflict and Mediation Event Observations (CAMEO) Event Codebook.

- Armed Conflict Location & Event Data Project (ACLED): Similar to the GDELT project, the ACLED database collects and categorizes information on conflict situations. The information mostly comes from local partners.

From our point of view, the codebooks of the GDELT and ACLED projects have their limitations as more categories are required to understand the complex interrelationships of events prevailing in peace operations. A prolonged drought in the area of operation can lead to water shortages resulting in social and military conflicts, and a fake post on a social network may bring peace operations into disrepute among the local population.

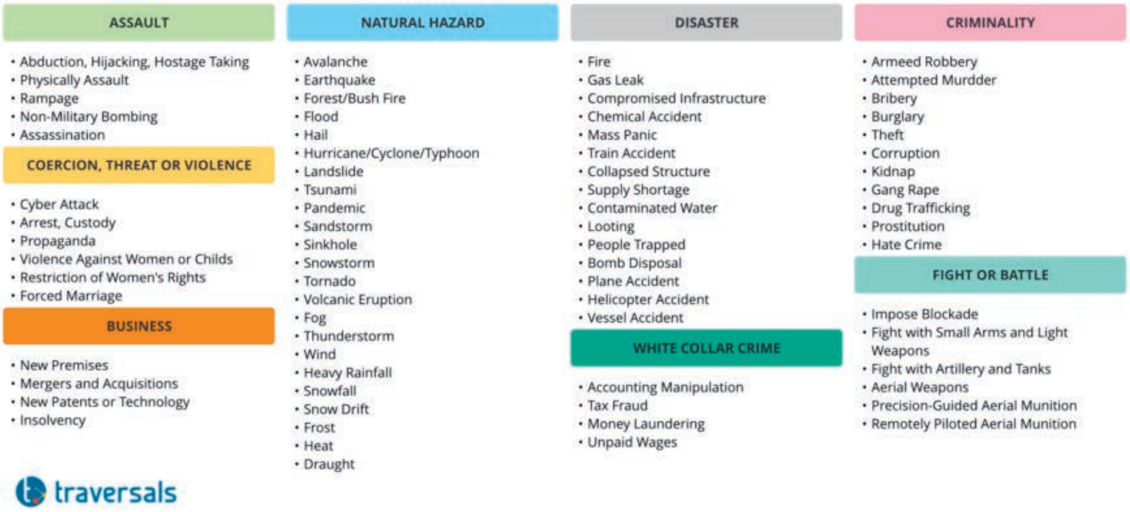
At the same time, a large number of problems must simultaneously be considered and also technically implemented in an efficient peace operations situational awareness environment, e.g., gender aspects, the protection of civilians, confidence-building measures, cultural property protection, propaganda awareness, children, and armed conflict, and women, peace, and security (UN Resolution 1325). To cover all these features of a crisis and to detect them as early as possible, it is essential to combine even more diverse event codebooks or protocols. As a first step, Traversals Analytics and Intelligence has taken ACLED and GDELT as a basis and extended them with other codebooks, such as:

- Management of a Crisis (MOAC): A vocabulary for describing disasters. It contains categories like Compromised Infrastructure.

- Common Alerting Protocol (CAP): A protocol for describing weather phenomena, e.g. heavy rain or heat.

There were no entries for these events in the existing codebooks. After experimenting over the last few months, we have developed a new event codebook that covers a huge variety of relevant situations, including also

- Supply chain law: violation of human rights, non-payment of wages, non-compliance with minimum social standards, child labor, etc.
- Protection of women and girls: sexual or other violence against women and girls, restriction of the rights of women and girls, forced marriage, etc.
- Freedom of the press: abduction or murder of journalists, prevention of freedom of the press, etc.



ASSAULT

- Abduction, Hijacking, Hostage Taking
- Physically Assault
- Rampage
- Non-Military Bombing
- Assassination

COERCION, THREAT OR VIOLENCE

- Cyber Attack
- Arrest, Custody
- Propaganda
- Violence Against Women or Childs
- Restriction of Women's Rights
- Forced Marriage

BUSINESS

- New Premises
- Mergers and Acquisitions
- New Patents or Technology
- Insolvency

NATURAL HAZARD

- Avalanche
- Earthquake
- Forest/Bush Fire
- Flood
- Hail
- Hurricane/Cyclone/Typhoon
- Landslide
- Tsunami
- Pandemic
- Sandstorm
- Sinkhole
- Snowstorm
- Tornado
- Volcanic Eruption
- Fog
- Thunderstorm
- Wind
- Heavy Rainfall
- Snowfall
- Snow Drift
- Frost
- Heat
- Draught

DISASTER

- Fire
- Gas Leak
- Compromised Infrastructure
- Chemical Accident
- Mass Panic
- Train Accident
- Collapsed Structure
- Supply Shortage
- Contaminated Water
- Looting
- People Trapped
- Bomb Disposal
- Plane Accident
- Helicopter Accident
- Vessel Accident

WHITE COLLAR CRIME

- Accounting Manipulation
- Tax Fraud
- Money Laundering
- Unpaid Wages

CRIMINALITY

- Armeed Robbery
- Attempted Murdder
- Bribery
- Burglary
- Theft
- Corruption
- Kidnap
- Gang Rape
- Drug Trafficking
- Prostitution
- Hate Crime

FIGHT OR BATTLE

- Impose Blockade
- Fight with Small Arms and Light Weapons
- Fight with Artillery and Tanks
- Aerial Weapons
- Precision-Guided Aerial Munition
- Remotely Piloted Aerial Munition

traversals

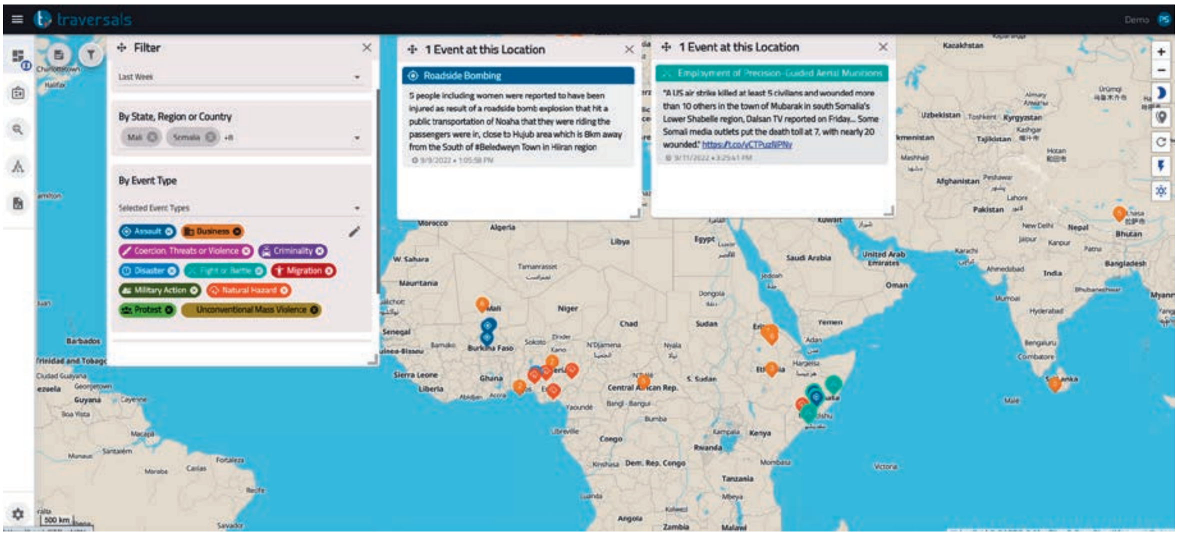
A FIRST REDUCTION OF THE DATA STREAM

As explained in the introduction, the objective is to better understand changes occurring in the area of peace operations as quickly as possible. To do this, PAI gathering needs to get as close as possible to where the action is. A so called Federated Search connects to various data sources, such as Google, Yahoo, Yandex, Naver, Bing, Ahmia, DuckDuckGo, Twitter, Reddit, Telegram, etc. persistently scanning multilingual texts, audio, images, and videos for the latest pertinent information. At the same time, peace operations do-no-harm rules must also apply to OSINT/SOCMINT: All information that could be used to identify sources, including but not limited to names and organizations, must be kept confidential or sanitized.

With the multitude of data sources subject to real-time demand, an incredibly large data stream is generated that is no longer possible to be manually evaluated. To cope with the problem, the integration of AI-based tools efficiently pre-evaluating and reducing the millions of daily puzzle pieces of information to a processable size is required to generate that data stream, a Federated Search connects to various data sources and automatically searches them at regular intervals, using simple, event-type specific keywords, in this case for peace operations. Unfortunately, more sophisticated searches are not yet possible, as they are presently not supported by most of the public available proprietery data sources.

100 Voices on Technology & Peace Operations

Taking the „Roadside Improvised Explosive Devise (IED)“ category from our event codebook as an example, we search for “Roadside IED“ in different languages on Google News or Twitter. Results in foreign languages are transparently translated by the Federated Search into English. The first processing also includes a Geocoding of text information, allowing a geospatial analysis of the findings. Looking at the results, you may see that a simple keyword search only reduces the data stream. However, a direct mapping of results to event types is not possible due to the linguistic ambiguity produced. It is the poor quality of the first results that is one of the big challenges when it comes to social media analysis for peace operations.



Roadside Bombing

5 people including women were reported to have been injured as result of a roadside bomb explosion that hit a public transportation of Noaha that they were riding the passengers were in, close to Hujub area which is 8km away from the South of #Beledweyn Town in Hiiran region

9/9/2022 • 1:05:58 PM

Employment of Precision-Guided Aerial Munitions

"A US air strike killed at least 5 civilians and wounded more than 10 others in the town of Mubarak in south Somalia's Lower Shabelle region, Dalsan TV reported on Friday... Some Somali media outlets put the death toll at 7, with nearly 20 wounded." https://t.co/yCTPuzNPNy

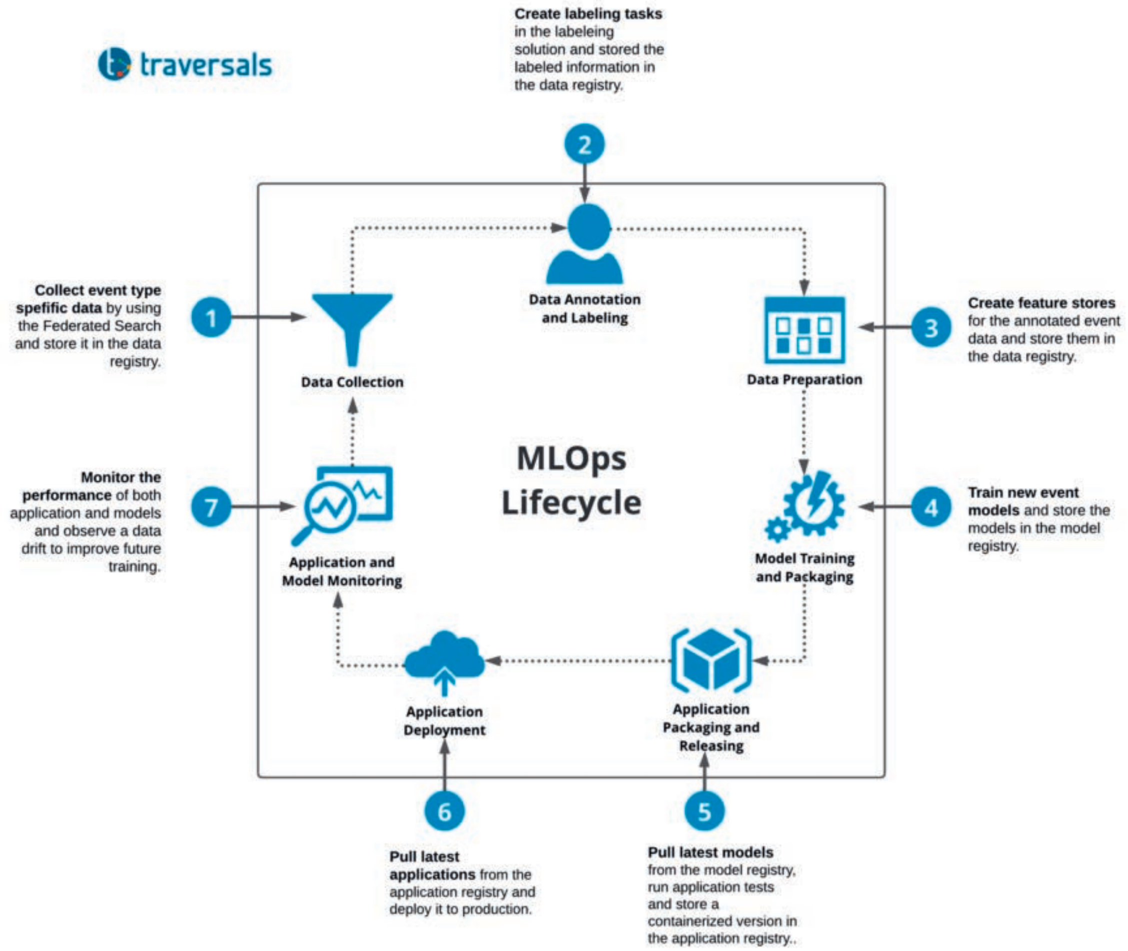
9/11/2022 • 3:25:41 PM

FINAL CLASSIFICATION WITH THE HELP OF NATURAL LANGUAGE PROCESSING

To do the final mapping of the initial low-quality results correlating them to the event types defined in the event codebook, we started to analyze the sentence structure including all words. This can be done intuitively by using state-of-the-art Natural Language Processing (NLP) libraries. Experiments showed that it is of crucial importance which verbs, nouns, adjectives, tenses, etc. were used in the text. As we labeled thousands of sample sentences, we could implement a robust feature extraction and feature classification for each event type. Our training set now contains over 3,000,000 entries, which are annotated sentence by sentence. Our own Federated Search allows us to expand this corpus daily, and adapt it whenever new event types are added to our extended codebook. After defining our event codebook and designing robust AI algorithms to map information to entries of this codebook, we faced new challenges:

- A new event codebook is constantly growing, and a training set is getting updated every day.
- It turned out that the creation of new AI models is not a static act, but a process that has to be operated daily.

In addition, the German Bundesamt für Sicherheit in der Informationstechnik (BSI) defined a new set of criteria for the secure use of machine learning methods in cloud services in 2021. The criteria in the Artificial Intelligence Cloud Service Compliance Criteria Catalogue (AIC4) addresses security and robustness, performance and functionality, reliability, data quality, data management, explainability, and bias. To get on top of this, we built a Machine Learning Operations (MLOps) pipeline that structures, optimizes, and makes the work more efficient and compliant with BSI AIC4. A summary of this can be seen in the diagram below. This MLOps pipeline is fully integrated into the architecture and allows daily, reproducible training of AI models for all entries of the event codebook. .


traversals
MLOps
Lifecycle
Data Collection
Data Annotation and Labeling
Data Preparation
Model Training and Packaging
Application Packaging and Releasing
Application Deployment
Application and Model Monitoring
1
2
3
4
5
6
7

Create labeling tasks in the labeleing solution and stored the labeled information in the data registry.

Collect event type spefific data by using the Federated Search and store it in the data registry.

Create feature stores for the annotated event data and store them in the data registry.

Monitor the performance of both application and models and observe a data drift to improve future training.

Train new event models and store the models in the model registry.

Pull latest applications from the application registry and deploy it to production.

Pull latest models from the model registry, run application tests and store a containerized version in the application registry..

KEY FINDINGS

PAI collection enables and improves the identification and monitoring of conflicts, and is essential for intelligence gathering during peace operations.

- PAI analysis is still a big challenge making it hard to get reliable and real-time situation reports.
- Systems to tackle these challenges are available, but they seem to be incomplete.
- AI-based analysis of OSINT introduces new capabilities, e.g. near real-time monitoring.
- Machine Learning Operations (MLOps) are required to deal with a constantly growing and self-adapting event codebook.
- The use of AI and OSINT will enhance peace operations' situational awareness and mitigate threats to a large extent.

ABOUT THE AUTHORS

Dr. Dirk Kolb is CEO and founder of Traversals Analytics and Intelligence, a German IT start-up specializing in AI-driven analysis of public information and social media for conflict monitoring and disaster response.

Philipp Starz is Business Development Manager at Traversals and brings his own operational experience from missions in Kosovo and Iraq.

REFERENCES AND FURTHER READING

- Abilova, O. & Novosseloff, A. (2016) Demystifying Intelligence in UN Peace Operations: Toward an Organizational Doctrine. New York: International Peace Institute.
- Carment, D., Rudner, M. & Heide, R. L. (2007) „Peacekeeping intelligence: extending partnerships and boundaries for peacekeeping", in Carment, D. und Rudner, M. (Hrsg.) Peacekeeping Intelligence: New players, extended boundaries. London: Routledge, pp. 31–44.
- de Coning, C. & Peter, M. (eds.) (2018) United Nations Peace Operations in a changing global order. Cham: Springer International.
- Dorn, A. W. (2010) United Nations Peacekeeping Intelligence. Oxford: Oxford University Press.
- Dorn, A. W. & Giardullo, C. (2020) „Analysis for peace: The evolving data tools of UN and OSCE field operations", Security and human rights, 31(1–4), pp. 90–101.

- Duursma, A. & Karlsrud, J. (2019) „Predictive peacekeeping: Strengthening predictive analysis in UN peace operations“, Stability International Journal of Security and Development, 8(1). doi: 10.5334/sta.663.
- Gilder, A. (2021) Stabilization and human security in UN peace operations. London: Routledge.
- Karlsrud, J. (2017) The UN at war: Peace operations in a New Era. Cham: Springer International Publishing.
- Karlsrud, J. (2014) „Peacekeeping 4.0: Harnessing the potential of big data, social media, and cyber technologies“, in Cyberspace and International Relations. Berlin, Heidelberg: Springer, pp. 141–160.
- Nikolic, S. (2017) “Open source intelligence in UN peacekeeping operations: An insight into perceptions and realities,” Vojno delo, 69(4), pp. 9–27.
- Nordli, D. & Lindboe, M. (2017) Intelligence in United Nations Peace Operations. Lillehammer: Norwegian Defence International Centre.
- Pauwels, E. (2020) Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention: Opportunities and Challenges for the International Community. Washington D. C.: Global Center.
- Rietjens, S. (2022) „NATO’s struggle for intelligence in Afghanistan“, Armed Forces and Society, pp. 1–12.
- Senekal, B. & Kotzé, E. (2019) „Open source intelligence (OSINT) for conflict monitoring in contemporary South Africa: Challenges and opportunities in a big data context“, African Security Review, 28(1), pp. 19–37.
- Steele, R. D. (2006) “Open Source Intelligence,” in Johnson, L. K. (ed.) Handbook of Intelligence Studies. Washington D.C.: Taylor & Francis, pp. 147–165.
- Wählisch, M. (2020) „Big data, new technologies, and sustainable peace: Challenges and opportunities for the UN“, Journal of Peacebuilding & Development, 15(1), pp. 122–126.
- Yankoski, M. u. a. (2021) „Artificial Intelligence for Peace: An Early Warning System for Mass Violence“, in Keskin, T. und Kiggins, R. D. (Hrsg.) Towards an International Political Economy of Artificial Intelligence. Cham: Palgrave Macmillan, pp. 147–175.