EPiC Series in Computing

Volume 102, 2024, Pages 172–177

Proceedings of Conference on Cognitive and Computational Aspects of Situation Management 2023

PINPOINT - A multidisciplinary framework for semi-automatic risk assessment in military operations and civilian missions

Gerhard Backfried[1], Dorothea Thomas-Aniola[1], Diego Pilutti[1], Martin Boyer[2], Rüdiger Hein[3], Amir Tabatabaei[3], Michael Zinkanell[4], Michael Suker[5], and Philipp Agathonos[6]

[1] HENSOLDT Analytics, Vienna, Austria
{gerhard.backfried,dorothea.thomas-aniola,diego.pilutti}@hensoldt.net
[2] Austrian Institute of Technology (AIT), Vienna, Austria
martin.boyer@ait.ac.at
[3] IGASPIN, Graz, Austria
rhein@IGASPIN.at, a.tatabaei@IGASPIN.at
[4] Austrian Institute for European and Security Policy, Vienna, Austria
michael.zinkanell@aies.at
[5] Austrian Ministry of Defence, Vienna, Austria
michael.suker@bmlv.gv.at
[6] Austrian Ministry of European and International Affairs, Vienna, Austria
philipp.agathonos@bmeia.gv.at

Abstract

We present the PINPOINT project aimed at designing a semi-automated risk assessment framework to support decision-making for military operations and civilian missions. These missions typically take place in critical international areas of remote countries with little infrastructure and require specific technical and operational support. To effectively plan and execute risk mitigation strategies, decision-makers require approaches for systematic, comprehensive risk analysis and proposals for measures. During the planning and execution phases, risk analysis must be updated regularly based on available information derived from Open Source data in combination with reliable and accurate Position-, Navigation- and Timing-Data (PNT) monitoring. The proposed framework focuses on innovations in the areas of a systematic risk analysis with derived mitigation actions, Open Source Intelligence (OSINT) related to these areas, Artificial Intelligence (AI) technologies for multiple types of sources (sensors, news, social media) and PNT monitoring based on GNSS-data analysis.

1 Introduction

The European Union (EU) is presently engaged in the execution of 18 military and civilian missions and operations [1], each designed to address critical issues in regions grappling with border-related challenges or conflicts. Among these missions, Austria participates in 8 operations, primarily focusing on regions burdened by crises. Given the complexity of the mission areas, a comprehensive risk analysis is required at the strategic, operational and tactical level. Mission regions pose considerable challenges, stemming from diverse ethical, socio-political, demographic, (human) rights, ecological, and technological factors. In particular, due to the limits of IT infrastructure the deployment of temporary, transportable technical security measures becomes imperative. In this context, open sources play a crucial role in stipulating pertinent data for monitoring the dynamic developments occurring within critical areas.

The PINPOINT project centers on the development of a methodology, complemented by a novel technical framework, geared towards the comprehensive collection, enrichment, and visualization of critical information for non-expert end-users to support them effectively and ensure the security of the stakeholders involved.

2 Outline of the Proposed Framework

In cooperation with the end-users of the project (Austrian Ministry of Defense and Foreign Ministry) a selection process is undertaken to identify a set of use cases. This selection guides the identification and collection of corresponding sources and relevant content. Subsequently, all data is ingested and enriched, making it available for analysis. To facilitate inspection and feedback by the end-users, a prototypical visualization framework will be employed. A set of indicators is to be designed and implemented, based on individual modalities. In a subsequent step, these will then be combined (fused) to produce multi-modal indicators, providing the basis for further insights and analysis. A set of interactive visualizations will enable end-users to effectively engage with the system, provide feedback and thus contribute to its refinement. Figure 1 presents an overview of the framework and approach.

The framework structure comprises four layers: dimension, category, indicator, and information. Dimensions represent the topmost entity describing the environment of the mission: geography, politics, society, economy, and infrastructure. Each dimension contains sub-dimensions divided into various categories, which in turn include indicators. For example, the first dimension “geography” is structured in five fine-grained categories topography, flora, fauna, geology, and climate, which contain between three and seven indicators (such as: rivers, lakes, oceans, mountains and relevant maps in the category topography). Through a combination of pre-existing quantitative and qualitative data, these indicators are filled with mission-specific information. The added value behind this approach lies in the scalability of the methodological framework, which can in principle be applied to any mission’s environment, providing tailored and demand-oriented information for individual and unique settings. To merge the methodological approach of scanning the mission’s environment by analysing relevant risks, the model encompasses two final dimensions – “conflict potential” and “hazard potential” – which identify threats on a societal and social-political level. Use-cases, which are developed and refined in close cooperation with the end-users, determine the geographic scope of sources, contents and language-dependent processing capabilities within the project. Processing and enrichment are divided into two strands of activities: those focusing on media ingested from open sources and

[1] EEAS Homepage – “Military and civilian missions and operations”, 17.03.2022, https://eeas.europa.eu/headquarters/headquarters-homepage

those concerning PNT and visual sensors. The former consist of a series of modules operating on different modalities of data, primarily on textual, audio and visual contents, which are enriched and converted into a set of indicators. Likewise, PNT and visual sensors are processed yielding a set of indicators. The scope and extent of these indicators will be determined in the course of the project by focusing on risk assessment and environmental analysis. To identify

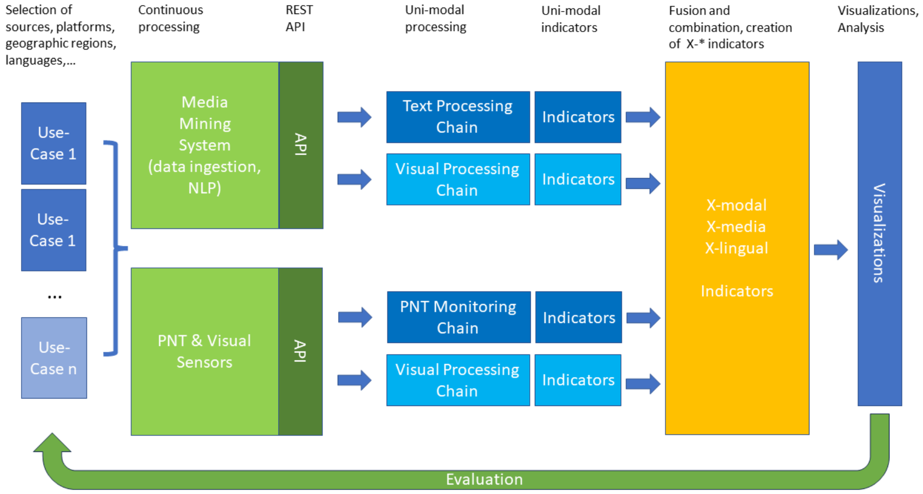

Figure 1: Overview of the PINPOINT framework and approach.

technical and non-technical risks and threats, the risk analysis method is founded on an initial scanning of the mission environment, facilitated by an interdisciplinary combination of social and political science, liberal arts, security studies, as well as ecological and economic factors. Special emphasis is placed on the inclusion of ethical considerations, gender issues, and cultural awareness into the analytical and methodological approach, not only to guarantee the depth of the mission environment analysis but also to ensure social, ethical, and ethnical inclusiveness and non-discrimination.

3 PNT Monitoring

Global Navigation Satellite Systems (GNSS) are essential for positioning and time applications across different realms, making Positioning, Navigation, and Timing (PNT) crucial in our daily lives. GNSS Radio-Frequency Interferences (RFI) including multipath, jamming, meaconing, and spoofing can deny or deceive GNSS services. Addressing these vulnerabilities with categorizations based on the impact and intention of the interferer is crucial for ensuring the reliability and integrity of GNSS systems across different sectors.

Figure 2 presents an overview of proposed architecture of the PNT-monitoring system.

Various methods for GNSS signal monitoring and interference detection have been proposed, but a comprehensive system for secure PNT has not been studied or implemented. The PINPOINT project aims to introduce a universal architecture incorporating multiple monitoring methods, including static stations, rover nodes with visual-enhanced systems, and rotating antennas. These nodes capabilities are combined in a novel manner to evaluate the GNSS signal

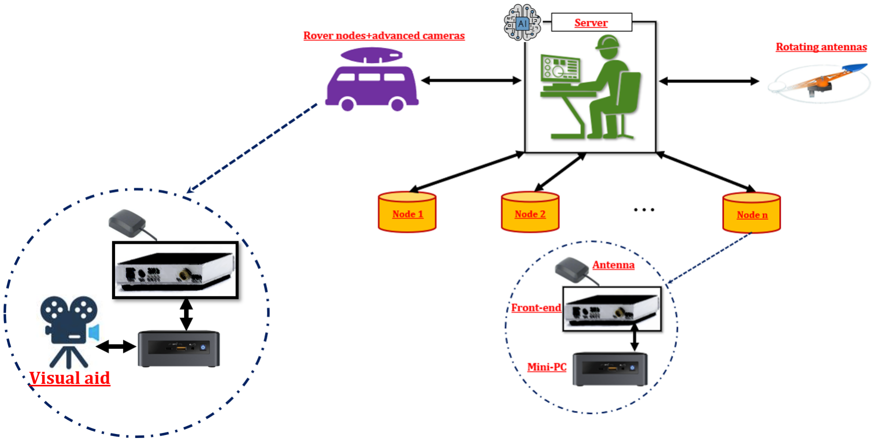

Figure 2: Overview of the proposed architecture of the PNT-monitoring system.

quality at the receiver stage, covering front-end samples, tracking units, and navigation solutions at server level. One innovation is a visual assistance (360 degree camera) unit installed on the rover nodes, which provides the possibility for the system to have a better comprehension of the environment by detecting hurdles for signal receiving. Distinguishing between multipath and spoofing as non-intentional and intentional interferences will decrease the rate of false alarms necessary for initiating further defensive reactions. In the PINPOINT project data from different nodes will be collected. To detect and characterize the interference in the desired area, an AI-based decision-making unit will be developed. Then, the server can identify the affected zone using the gathered information and especially the directions provided by the rotating antennas. This project aims to provide an all-in-one solution for PNT monitoring, contributing to the advancement of knowledge in this field.

4 OpenSource Intelligence

Open Source Intelligence (OSINT) as part of an all-source strategy or as a supplement to other intelligence methods such as SIGINT (Signal Intelligence) or HUMINT (Human Intelligence) has been a recognized means of obtaining information for some time [1]. The ensuing scheme of All-Source Intelligence comprises all available sources that can be used to gather and confirm information. Technological advances and an exponential increase in users have led to the situation that some organizations in the security field already work primarily with OSINT (e.g., the UN and OSCE use OSINT in peacekeeping missions [2]). However, in many cases a lack of a consistent application of OSINT and a clear methodology for its use can be identified. Within PINPOINT, the HENSOLDT Media Mining System, a state-of-the-art OSINT system [3] is employed to collect and process structured and unstructured data from a set of publicly available sources according to mission-specific requirements. Contents are enriched with a range of technologies from the field of Natural Language Processing (NLP) and Computer Vision (CV), stored and made available for later analysis and visualization. Furthermore, the system will provide enriched data as input for the creation of multi-modal indicators. These are in turn envisioned to be combined with further indicators derived from other kinds of processing and sources, e.g., PNT-monitoring. Overall, a methodology based on the NATO OSINT Cycle[2] is followed to provide a principled approach for all steps mentioned above.

5 Information Fusion

In order to improve the extent and reliability of information and/or to detect tampering and disinformation, an approach based on combined and fused indicators will be applied. This approach aims to produce more robust and reliable information compared to any of the individual indicators alone. Furthermore, it allows for future extensions regarding fusion with information from further sources. The combination of indicators and sources and the resulting visualization and analysis capabilities are envisaged to provide additional insights over the analysis of individual indicators alone and thus allow the detection of anomalies and cross-checking of information.

The generation of complex indicators and insights form an essential ingredient for the utilization of the analysis results. Different techniques and methods will be adopted. Strongly linked attributes are particularly valuable for detecting the non-explicit associations in the dataset [4]. Organizations within the project will be able to combine non-OSINT data with OSINT data, achieving significant additional value in terms of saturation [5]. Establishing heterogeneity and AI-enabled aggregation within an all-source data fusion paradigm is a key goal for OSINT in PINPOINT. According to the use-cases, it is planned to establish datasets corresponding to the strands of processing.

6 Current state, planned activities and outlook

The project started in Feb 2023. Since then, the use-cases and scenarios have been fixed in cooperation with the end-users, corresponding to two relevant CSDP missions of the Austrian Armed Forces. Based on a principled approach developed within previous projects [6], the locations involved in these scenarios and relevant open sources have been identified, a set of NLP modules has been extended for increased coverage (e.g. for the detection of locations named in media) and continuous collection and processing of contents has begun. The resulting dataset will serve both, training as well as evaluation purposes within the project. In parallel, state-of-the-art AI-based algorithms and models are being developed resulting in improved resilience, robustness, and security for PNT solutions employed in the scenarios. A risk assessment model accommodating OSINT and PNT and encompassing various risk-dimensions is being developed and refined. Based on this model, a set of media based indicators will be derived. These indicators will first be combined in a cross-media, cross-platform and cross-lingual manner and subsequently be fused with indicators derived from PNT-monitoring. Both strands of indicator development will proceed in parallel on both use-cases and in tandem with work regarding risk-assessment. Feedback from end-users will be gathered in evaluation sessions and integrated. Eventually, these indicators are to be used within risk-assessment methods employed by the end users for both, military and civilian missions. Project results are expected to be integrated in OSINT and PNT solutions of the industry-partners, extending and enhancing current product portfolios.

[2] https://www.natoschool.nato.int/Academics/INTEL

Acknowledgments

PINPOINT is partly funded by the Austrian Security Research Programme KIRAS of the Austrian Federal Ministry of Finance (BMF). The authors would like to thank Marcin Skowron for his valuable inputs and assistance.

References

[1] H. J. Williams and I. Blum, *Defining second generation open source intelligence (OSINT) for the defense enterprise.* Rand Corporation Santa Monica, 2018.

[2] A. W. Dorn and C. Giardullo, “Analysis for peace the evolving data tools of un and osce field operations,” *Security and Human Rights*, vol. 31, no. 1-4, pp. 90–101, 2020.

[3] G. Backfried, C. Schmidt, M. Pfeiffer, G. Quirchmayr, and J. Göllner, “Open source intelligence for traditional- and social media sources,” in *Proceedings of the 10th International Conference on e-Business*, 2015.

[4] K. Mak, H. Pilles, J. Göllner, and J. Klerx, *Wissensentwicklung mit ”CROWD OSInfo” : eine Innovation des Cyber Documentation & Research Center (CDRC) der Zentraldokumentation (Zent-Dok), Landesverteidigungsakadmie (LVAK)*, ser. Schriftenreihe der Landesverteidigungsakademie. Republik Österreich / Bundesministerium für Landesverteidigung, 2015. [Online]. Available: https://books.google.at/books?id=2V2lzgEACAAJ

[5] T. Day, H. Gibson, and S. Ramwell, “Fusion of osint and non-osint data,” *Open source intelligence investigation: From strategy to implementation*, pp. 133–152, 2016.

[6] G. Backfried, L. Bettili, A.-L. Dudenhöfer, M. Rohm, F. Pieralice, and F. Britti, “Open source intelligence for traditional- and social media sources,” in *Proceedings of the Intelligence 2023 Conference of the Australian Institute of Professional Intelligence Officers, forthcoming*, 2023.