OCTOBER 16-17, CHALKIDIKI, GREECE 2024

RISE-SD 2024 CONFERENCE

RISE SD 2024

Research and Innovation Symposium for European Security 2024

Proceedings Book | Online edition

RISE-SD 2024
CONFERENCE

October 16-17, Chalkidiki, Greece

FOREWORD

We are pleased to introduce these proceedings of the Research and Innovation Symposium for European Security 2024 (RISE-SD 2024).

RISE-SD 2024 is a European Research and Innovation Conference focused on presenting and demonstrating technologies, frameworks, methodologies and results of EU Research and Innovation projects in the fields of Fighting Crime and Terrorism, Disaster and Crisis Management, Critical Infrastructure Protection, Cybersecurity, and Border Management, among others.

The extended abstracts in these proceedings are linked to the presentations given during the conference and examine several aspects of security and defence challenges, as well as the related cutting-edge technologies and strategies being developed to address them.

We would like to thank all contributors to these proceedings for their hard work and dedication towards advancing EU Security Research and Innovation.

The RISE-SD2023 Organising Committee

CO-ORGANISING PROJECTS

Acting – Advanced Cybersecurity Training

ENACT – European Network Against Crime and Terrorism

LAGO

TENACITy

ATLANTIS

encrypt

MULTIRATE

TESSERA

CASSATA

EURMARS

ODYSSEUS

TESTUDO

CESAGRAM

FALCON – Fighting Corruption & Organised Crime

ODYSSEUS

TREEADS

FaRADAI – Frugal Robust Advanced Intelligence

PERIVALLON

CONNECTOR

FERMI – Fake News Risk Mitigator

SAFEGUARD

VANGUARD

CUIIS

FIBERMARS

STARLIGHT – Sustainable Autonomy and Resilience for LEAs using AI against High Priority Threats

VANOS – Your trusted partner.

ELECTRON

INHERIT

TEAMUP CBRN-E

WEMOR

CORE ORGANISING GROUP

iti – CENTRE FOR RESEARCH & TECHNOLOGY - HELLAS
Information Technologies Institute

www.iti.gr

M4D – MultiMoDal Data Fusion and Analytics Group

www.m4d.iti.gr

satways

www.satways.net

www.di.mod.bg

With the participation support of

European Commission

DG Home, CERIS, REA

Contents

01. Better Protect the EU and its Citizens against Crime and Terrorism

CESAGRAM:

AI-based technologies Towards the Prevention and Detection of Grooming Content Online

Theoni Spathi[1], Nikolaos Mylonas[1], Nikolaos Stylianou[1], Athanasios Batsioulas[1], Christos Theodosiadis[1], Ourania Theodosiadou[1], Despoina Chatzakou[1], George Kalpakis[1], Theodora Tsikrika[1], Stefanos Vrochidis[1]

[1] Information Technologies Institute, Center for Research and Technology Hellas

Keywords

Online grooming, AI-based technologies, Natural Language Processing, Risk Assessment

Extended Abstract

Online grooming has been widely used by offenders to lure children and further sexually exploit and abuse them. The fight against online Child Sexual Abuse and Exploitation (CSAE) is one of the most crucial priorities of the EU agenda, as CSAE is one of the fastest growing criminal activities. The recent Eurobarometer Survey on the protection of children against child sexual abuse (European Union, 2023) underlines that the vast majority of Europeans (73%) believe that child sexual abuse occurs on the internet on a regular or very regular basis, and 92% concur that children are becoming more and more vulnerable to dangers online. According to the latest annual report of the Internet Watch foundation (2022), a total of 255,588 reports (out of the 375,230 assessed), contained child sexual abuse imagery, with a 60% increase in 7-10 years old and 20% of Category A (depicting serious abuse). In addition, Europol's Internet Organised Crime Threat Assessment - IOCTA (2024) underpins the evolution of the threats posed in the area of CSAE, that is triggered not only by the uptake of new technologies and the use of Artificial Intelligence (AI) by offenders, but also by the unsupervised presence of children online, especially in social media platforms, the users of which are exponentially increasing (Petrosyan, 2024). Anecdotal evidence from Missing Children Europe's 116000 hotlines has shown a concerning correlation between online grooming activities and incidents of missing children, highlighting the need for more research to enable effective responses to such phenomena, including AI-based tools and technologies ready to assist towards the prevention and detection of grooming content online, facilitating the work of law enforcement.

CESAGRAM (Towards a Comprehensive European Strategy Against tech-facilitated GRooming And Missing) is a two-year European Funded project (January 2023-December 2024) which aims at tackling online child sexual exploitation and abuse through enhancing the understanding of the process of grooming, and more particularly the way it is facilitated by technology, as well as its link to CSAE and missing-children's cases, a currently under-researched area. During the lifespan of the project, targeted training and awareness raising tools, along with a gamified educational platform for awareness raising have been developed, with particular attention to the identified needs and requirements of the relevant end users, while empirical research with CSAE survivors has further advanced the proposed preventive campaign, emphasising in parallel on specific policy recommendations.

One of the main outcomes of the project has been the development of a set of AI-based tools, which aim to facilitate the prevention and detection of grooming content online. After appropriate monitoring of online spaces for grooming-related content, Natural Language Processing (NLP), including Named Entity Recognition (NER), Sentiment, Emotion, Taxonomy Classification, and Authorship Analysis are applied. In particular, NER extracts entities and key concepts from the gathered data, Sentiment Analysis evaluates the content to determine its overall sentiment, and Emotion Analysis categorises the text into one of six basic emotions. In addition, Taxonomy Classification categorises the text with respect to a taxonomy related to grooming. All NLP outputs are then leveraged by the Risk Assessment tool to identify potential grooming behaviours by estimating the risk of grooming behaviour and providing real-time alerts. Finally, the Authorship Analysis links distinct user accounts that potentially belong to the same individual-physical person. In that way, useful intelligence is being generated to combat child grooming, further enhancing the operational capabilities of the relevant law enforcement agencies. All the developed tools have been integrated into the CESAGRAM Dashboard, a user-friendly interface that offers various capabilities, including data gathering, a comprehensive view of gathered data along with insights from the NLP tools, and interactive visuals. Our overall goal is to provide a complete and effective solution both to end users for accurately responding to any grooming incident online and to the scientific community for the future development of innovative responses in this field of research.

Acknowledgements

This project was funded by the European Union's Internal Security Fund under Grant Agreement No. 101084974. The content of this article represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

References

1. European Union. (2023, July). Flash Eurobarometer survey on "Protection of Children against Online Sexual Abuse". Retrieved from https://europa.eu/eurobarometer/surveys/detail/2656
2. Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
3. Internet Watch Foundation. (2022). The Annual Report 2022 - #BehindTheScreens. Retrieved from https://annualreport2022.iwf.org.uk/wp-content/uploads/2023/04/IWF-Annual-Report-2022_FINAL.pdf
4. Petrosyan, A. (2024). Worldwide digital population 2024. Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/

EITHOS:

European Identity THeft Observatory System

Eleana Almaloglou[1], Kostantinos Kostandoudakis[1], Georgios Petmezas[1], Dimitrios Zarpalas[1]

[1] Center for Research and Technology Hellas

Keywords

Deepfake, Online Identity Theft (OIDT), Authentication Technology, Digital Forensics

Extended Abstract

Identity Theft

Identity theft has impacted individuals personally and professionally for centuries, from physical impersonation and document theft to forgery. The goal is to impersonate a victim to gain access to funds, restricted areas, contacts, or sensitive information. As identity documents became more formalized and everyday activities increasingly automated, the scope of identity theft has expanded.

In the digital age, many personal and professional activities now occur online—communication, banking, file sharing, and more. This shift has given rise to Online Identity Theft (OIDT), where attackers impersonate victims to access personal data. OIDT often has more immediate and far-reaching effects than traditional identity theft and is harder to detect, as it relies on digital identifiers like passwords, avatars, and text-based communications. The rise of advanced technologies like deepfakes has further complicated this, allowing attackers to manipulate digital images and videos, making it easier to deceive and harder to identify impostors.

EITHOS

EITHOS - the European Identity Theft Observatory System - is a Research and Innovation project funded by the European Commission under the Horizon Europe Framework Programme. EITHOS aims to counter OIDT by informing and educating citizens on the dangers of OIDT and how to protect against it, and by identifying and addressing the challenges that police authorities face against it. In particular, it is taking action in four distinct areas:

1. Socio-psychological: Studying the impact of OIDT on its victims and society, assessing the support structures that are in place and recommending pathways to improve them.
2. Technological: Researching and implementing tools for law enforcement authorities to assist them in identifying innovative methods of OIDT such as deepfakes and social media botnets, while also providing a tool to extract useful trend information from deep or dark web forums.
3. Legal: Studying the current practices on e-evidence collection and exchange, assessing current legislation impacting OIDT and recommending future improvements.
4. Citizen Awareness: Reaching out to inform and educate citizens in a wide range of formats, including articles, workshops, public events, quizzes, games, and comics.

Deepfakes

Recent advances in deep learning have allowed the fully- or semi- automatic generation or manipulation of media content. Deepfakes are images, videos or sound clips that are manipulated by deep learning techniques so as to alter the identities - in particular faces and voices - of the people depicted in them [1]. Especially in the last couple of years, deepfakes have the capacity to be so realistic as to pass casual inspection, and often a more detailed inspection as well [2]. While the best quality currently needs some extra time and some human fine-tuning, passable deepfakes are feasible in real-time as well.

In the context of OIDT, deepfakes can be a powerful tool in a fraudster's arsenal. It is human instinct to believe what we see and hear, and deepfakes can impersonate a victim in online media or live streams, leading to scams, but also defamation, blackmail, or the spread of fake news.

Video deepfake detection

Following the rise of deepfakes, deepfake detection methods have emerged as well. Video deepfakes are often prone to tell-tale distortions, blurrings, artifacts or other inconsistencies, and such methods utilize deep learning approaches, including CNNs and RNNs, to detect them [3,4].

However, the supervised learning approach many of those methods use means that they are dependent on the availability of large datasets of both genuine and deepfaked data - and, by necessity, they will learn to identify the specific quality and distortions particular to the deepfake creation methods used to create such data. This can lead to overfitting and a lack of generalizability across different datasets [5], while implying that such approaches might not perform well against new or upcoming deepfake creation tools.

To address this challenge, EITHOS is researching a novel approach to video deepfake detection that focuses on the underlying 3D structure of the face in a video under consideration, comparing it with the structure of the face in one or more reference videos. Hence, it follows a verification rather than a detection approach, effectively transforming the question "is this a deepfake?" into the equivalent "is this the same person as in the reference?"

The proposed method uses 3D Morphable Models (3DMMs) to extract facial biometrics from input videos, feeding this data into a hybrid CNN-LSTM-Transformer model. This model learns unique features of a target identity, allowing it to detect manipulations by comparing them to authentic benchmarks. Trained solely on pristine data, the model is agnostic to manipulation techniques, enhancing its ability to distinguish real content from deepfakes.

This approach only requires unmanipulated videos for training, and hence it does not run the risk of overfitting to a particular deepfake creation methodology, leading to greater generalizability across different types of deepfakes. In addition, it is also efficient in terms of computational requirements and speed. Early results show a strong performance across a range of video compression levels, quality settings and types of manipulation.

Acknowledgements

This work has been supported by the European Commission funded program EITHOS, under Horizon Europe Grant Agreement 101073928.

References

1. Yu, P., Xia, Z., Fei, J., & Lu, Y. (2021). A survey on deepfake video detection. Iet Biometrics, 10(6), 607-624.
2. Verdoliva, L. (2020). Media forensics and deepfakes: an overview. IEEE journal of selected topics in signal processing, 14(5), 910-932.

3. Rana, M. S., Nobi, M. N., Murali, B., & Sung, A. H. (2022). Deepfake detection: A systematic literature review. IEEE access, 10, 25494-25513.

4. Malik, A., Kuribayashi, M., Abdullahi, S. M., & Khan, A. N. (2022). DeepFake detection for human face images and videos: A survey. Ieee Access, 10, 18757-18775.

5. Cozzolino, D., Rössler, A., Thies, J., Nießner, M., & Verdoliva, L. (2021). Id-reveal: Identity-aware deepfake video detection. In Proceedings of the IEEE/CVF international conference on computer vision (pp. 15108-15117).

EMPOWER:

The Challenge of the absorption of AI enabled tools by European Law enforcement: The EMPOWER project

Shona Linehan[1], George Kalpakis[2], John Mulcahy[3], Martin Mullins[4]

[1] **Transgero and University of Galway,** Ireland

[2] **Information Technologies Institute, Centre for Research and Technology Hellas,** Thessaloniki, Greece

[3] **Transgero,** Ireland

[4] **Transgero and University of Limerick**

Extended Abstract

Introduction

From the outset of the EMPOWER project, the emphasis has been on deployment. The consortium is charged with bringing forth the outputs from previous EC funded projects in this domain and adapt the tools developed to be ready for deployment. Implied in this task is the raising of TRL levels and/or some of the metrics produced by the multiRATE project[1]. The EMPOWER project is made up of law enforcement agencies, tool developers, research technological organisations, legal and ethical experts and is led by a campus company with origins in a business school. The paper presented at the RISE event[2] will describe the approach and the outputs of the EMPOWER project. At the same time, we will adapt a conceptual framework (institutional logics) to explain some of the challenges faced in the testing and deployment of the 8 tools.

The overall goal of EMPOWER is to foster the uptake of innovative solutions based upon AI powered tools allowing LEAs to increase their capabilities in investigative fields including Child Sexual Exploitation (CSE), Terrorism, Cybercrime and the protection of Public Spaces. Over the 2-year lifespan of the project, EMPOWER will deploy and pilot test a total of 8 investigative tools in the fields of Image/Video, Voice/Text and Federated Learning.

Context

Digitization and algorithmic regimes, such as the datafication of citizens' activities, emotions and social relations, and risk profiling across multiple domains signal important changes at a societal level. This academic paper is located this in the specific domain of policing. That said, it is important to factor in the heterogenous nature of this area. The end users of digital tools work in different areas of policing – each with its own identity, networks and institutional history. These communities of end-users would include forensics, financial investigation units (FIUs) as well as investigators. Worthy of note also are the distinct structures of police forces in Europe which include those with a more civilian ethos and those with a more para-military orientation. To some extent, this explains some of the frictions encountered in the introduction of new technologies and practices into police forces. The EC has been funding collaboration between tool providers and law enforcement agencies (LEAs) for more than a decade and yet technological absorption remains problematic. This paper examines some of the dynamics around this and will leverage the literature of institutional logics to interrogate the issues around these

[1] For more details see https://www.multirate.eu/
[2] See, https://rise-sd2024.eu/

processes.

Theoretical Lens

With its origins lying in institutional theory, Institutional Logics (IL) provides a method for better understanding the core values and indeed the "ways of working" of a particular grouping (in this case – LEAs). It can give structure to the explanation of rationales behind actions. In this case, the value for this approach lies in the facilitation of an understanding of institutional practices in policing that may hinder new technology adoption. Moreover, IL allows for a more comprehensive understanding of cultural dynamics within organisations. The strength of IL resides with its ability to move beyond a more reductive analysis of behaviour. Thus, Institutional logics has offered some important insights into processes of change within large organisations. In this particular domain, we see Wathne (2020) making use of IL based theoretical perspectives in order to gain insights into improving practices among LEA professionals.

The EMPOWER project

The widespread nature of criminality in the digital space presents a serious challenge to police and security services. EMPOWER addresses the problem with a focus on the tools and skillsets required to tackle this phenomenon. Moreover, for police management it implies the need for new types of professional formation and training – an important element of EMPOWER resides in its training assessment piece. This paper is based on the authors' experience in managing and participating in two EC funded projects which sought to develop new AI driven tools for use in European police forces. In one instance (EMPOWER) the authors were part of the team coordinating the project and in the other (ANTIFINTER), the authors worked on training and policy related deliverables.[3] That said, the emphasis here is on the EMPOWER project.

EMPOWER is a Digital Europe project, a new funding scheme created by the European Commission acknowledging the need to focus on deployment and adoption of digital technologies. EMPOWER has two core unique aspects – firstly, it is specifically building upon developments made in previous Horizon Europe projects working to ensure successful uptake of their AI tools by European Law Enforcement Agencies (LEAs). [4] EMPOWER is also working with two LEAs to encourage cross border co-operation. To sum up work on the tools, these exist in 3 areas; image/video, voice and text and federated learning. Overall EMPOWER is charged with demonstrating solutions that provide usability, efficiency, training and compliance within EU standards as regards privacy and data protection.

Regulatory and Legal Backdrop

This is a high-stakes environment and highly consequential in terms of the operation of the State and its interaction with wider society. In terms of the legal regulatory picture, the recent AI Act denotes the use of AI by law enforcement (in some instances) as high-risk.[5] The EU's Police Directive is also an important reference point. Furthermore, there are other relevant legal structures including GDPR, national legal regimes and legal precedent emerging from courts across Europe. Wider societal acceptance is also an important part of the picture. EMPOWER has a dedicated work package to deal with these issues.[6] From an implementation perspective, the ethico-legal background does present an additional challenge to the consortium and has resulted in the creation of bespoke governance procedures.

Discussion and some preliminary conclusions.

All this implies a new "lifeworld" for police officers in which more resources and attention are dedicated to emerging domains of AI and big data. This is not to say that police organisations do not have a long track record of bringing in new technology but rather it is a question of degree. There is a new dispensation emerging whereby policing is becoming **datafied** and such practices as machine learning (one form of AI) will be more important. Further along this scale are decision making tools in the justice system. This is not a simple technical or managerial challenge, cultural, institutional and social factors are important variables. Thus, there are different classes of challenge to overcome in the roll-out of these AI driven tools and technologies. Firstly, there are the technical challenges in creating tools and creating efficient data pipelines. Secondly, there are governance issues that relate to hard law, applied ethics and societal acceptance. Thirdly, there are the institutional factor within LEAs that may hinder the adoption of these tools.

References

Selected Bibliography

1. AP4AI, (2023), International Citizen Consultation on AI Accountability in Policing.
2. European Union Agency for Law Enforcement Training (CEPOL) (2019), Operational Training Needs Analysis Cybercrime – Attacks against Information Systems
3. European Union Agency for Law Enforcement Training (CEPOL) (2020), Operational Training Needs Analysis Criminal finance, money laundering and asset recovery
4. Harkin, D. and Whelan, C., 2022. Perceptions of police training needs in cyber-crime. International Journal of Police Science & Management, 24(1), pp.66-76.
5. Liou, K.T., 2019. Technology application and police management: issues and challenges. International Journal of Organization Theory & Behaviour, 22(2), pp.191-208.
6. Sunde, N. and Dror, I.E., 2019. Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. Digital investigation, 29, pp.101-108.
7. Wathne, C.T., 2020. New public management and the police profession at play. Criminal Justice Ethics, 39(1), pp.1-22.
8. Weiskopf, R. and Hansen, H.K., 2023. Algorithmic governmentality and the space of ethics: Examples from 'People Analytics.' human relations, 76(3), pp.483-506.
9. Wilson, D., 2019. Platform policing and the real-time cop. Surveillance & Society, 17(1/2), pp.69-75

[3] See https://anti-finter.eu/ and https://transgero.eu/empower/
[4] These EC funded projects include STARLIGHT, GRACE, DANTE, AND AIDA.
[5] For a summary see https://artificialintelligenceact.eu/high-level-summary/
[6] This is led by · ICT LEGAL CONSULTING – STUDIO LEGALE ASSOCIATO BALBONI BOLOGNINI & PARTNERS – ICTLC

FALCON:

A Data-driven Risk Assessment Tool for Enhancing Anti-Corruption Measures through Real-time Predictive Analytics

Nikolaos Peppes[1], Theodoros Alexakis[1], Emmanouil Daskalakis[1], Konstantinos Demestichas[2], Evgenia Adamopoulou[1]

[1] **Institute of Communication and Computer Systems,** Greece,

[2] **Department of Agricultural Economics and Rural Development,** Agricultural University of Athens, Greece

Keywords

Risk Assessment, Predictive Analytics, Corruption, Anti-corruption, Risk Classification, Decision Making

Extended Abstract

The paper introduces the Advanced Corruption Risk Assessment (ACRA) tool, a cutting-edge solution designed to enhance the detection, management, and prevention of corruption through real-time predictive analytics. Developed under the FALCON project, ACRA leverages advanced machine learning algorithms and predictive models to provide data-driven risk assessments, enabling law enforcement agencies and anti-corruption authorities to identify high-risk corruption cases with greater accuracy and efficiency. The tool's core capabilities include anomaly detection, real-time monitoring, and both quantitative and qualitative assessments using multiple computational mechanisms, offering a comprehensive approach to addressing corruption risks. ACRA's architecture integrates corruption indicators from diverse multivariate data sources, including financial transactions, procurement records, and cross-border financial flows, providing a holistic view of corruption threats. In summary, the work highlights the key features of ACRA, its technical framework, and the transformative impact it has on corruption risk management.

Introduction

Corruption is a significant challenge that undermines economic, social, and political stability across Europe. More specifically, according to the Eurobarometer report in 2023 (European Commission, 2023), 70% of the survey participants believe that corruption is widespread in their country and 64% believe that corruption is unacceptable. Also, above 70% think that corruption is widespread in national public institutions and that the direct links between businesses and politics leads to corruption. On the contrary, only 32% of the participants are convinced that the prosecutions against corruption are adequate.

The ability to measure and detect corruption is inherently difficult as there is no single formula and one-size-fits-all approach as well as no single indicator that could capture the multidimensional aspect of corruption. Moreover, all indicators and existing measurements of corruption are biased towards a specific dimension of corruption or towards a specific country or region (Hamilton & Hammer, 2018). Thus, the ability to detect and mitigate corruption risks in real-time is crucial for maintaining transparency and integrity within society. Traditional anti-corruption efforts have often struggled to keep pace with the sophisticated and evolving nature of corruption schemes, particularly in complex environments such as public procurement and cross-border financial transactions. Thus, FALCON's Advanced Corruption Risk Assessment (ACRA) tool aims to bridge the existing gaps in existing approaches of fighting corruption by engaging heterogeneous data-sources and analyzing different dimensions of corruption.

The Advanced Corruption Risk Assessment (ACRA) tool

The Advanced Corruption Risk Assessment tool, being developed as part of the FALCON project, represents a major advancement in the fight against corruption. ACRA is specifically designed to support law enforcement agencies (LEAs) and anti-corruption bodies by providing a robust, data-driven platform for risk assessment and investigation prioritization. By integrating state-of-the-art machine learning algorithms with real-time data processing, ACRA offers a proactive approach to identifying and responding to corruption risks.

The ACRA tool's strength lies in its ability to analyse vast datasets in real or near-real-time, detecting patterns and anomalies that signal potential corruption. It incorporates both supervised and unsupervised learning models, enabling the tool to learn from historical data and adapt to new and emerging corruption threats. Additionally, ACRA assesses both quantitative and qualitative risk factors, such as the discretionary authority of officials or the level of transparency in specific processes, providing a more nuanced understanding of corruption risks.

The architecture of ACRA is designed to facilitate seamless data integration, allowing it to process information from multiple sources, including financial records, procurement logs, and unstructured textual reports. The tool's backend services, built on a Flask framework, ensure efficient data handling, while the RESTful API layer supports real-time communication between data processing components and the user interface. The graphical user interface (GUI) offers a user-friendly platform where investigators can interact with risk indicators, analyse trends, and receive alerts for high-risk activities. ACRA provides to the end-users a traffic light-style principle (Sabari, 2022) representation by calculating the probability of a corruption incident. More specifically, as shown in Figure 1, an interactive matrix updated in real or near real-time allows the end-user to instantly detect incidents. The system categorizes these incidents as very likely (red colour), or likely (yellow/orange colour) or not likely (green) to result in corruption.

As shown in Figure 1, the columns indicate the probability of an incident to lead to corruption, while the rows represent the severity of the suspected corruption event. Thus, the upper right corner highlights critical corruption incidents whilst the lower left corner reflects less severe, unlikely cases.

Conclusions

Bridging the gaps in a multidimensional domain such as the fight of corruption is a highly demanding task. In this light, ACRA provides a comprehensive solution for detecting, managing, and preventing corruption by combining advanced analytics, predictive algorithms, and qualitative assessments. Its innovative approach not only enhances the efficiency of anti-corruption efforts but also shifts the focus from reactive investigations to proactive prevention, ensuring that high-risk activities are flagged in real-time and addressed before they escalate. As corruption schemes become increasingly sophisticated, tools like ACRA will play an

essential role in safeguarding transparency and accountability in public and private sectors.

Acknowledgements

Co-funded by the European Union within the Horizon Europe programme, under grant agreement No. 101121281 (FALCON). Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

1. European Commission. (2023). Citizens' attitudes towards corruption in the EU in 2023. European Commission. doi:10.2837/5674
2. Hamilton, A., & Hammer, G. (2018, 01). Can We Measure the Power of the Grabbing Hand? A Comparative Analysis of Different Indicators of Corruption. Retrieved from World Bank Group: https://openknowledge.worldbank.org/entities/publication/18ca9e5c-a5f6-59ec-9937-8cbb5033b601
3. Sabari, K. S. (2022). Red Light, Green Light and Amber Light Theories of Administrative Law: A Comprehensive Analysis. Indian Journal of Law and Legal Research, 4(4). Retrieved from https://www.ijllr.com/post/red-light-green-light-and-amber-light-theories-of-administrative-law-a-comprehensive-analysis

Figure 1: Real time risk assessment matrix concept

FERMI:
Facilitating the Fight against Disinformation-induced Violent Crimes

Sven-Eric Fikenscher[1]

[1] **Bavarian Police Academy,** Germany

Keywords

Disinformation, Violent Crime, Social Medias

Extended Abstract

In recent years, a drastic rise in the spread of disinformation has been witnessed globally, especially in the Western world. Whilst the public discourse about the implications of disinformation campaigns has mostly centred around foreign manipulation efforts (Russian activities aimed at undermining Western elections are a case in point) (EUvsDisinfo, 2024), the spread of disinformation is taking a growing toll on domestic security.

The digital revolution has given anyone that aspires to spread false allegations a new tool to get their message across. The nexus between the spread of disinformation on social media and violence was powerfully illustrated by the events in Washington, D.C. on 6 January, 2021 when a mob of Trump supporters, driven by devious claims about the election being stolen from their candidate, stormed the U.S. Capitol to prevent the certification of Joe Biden's ballot box win (Jones, I. and Comerford, M., 2023). Disinformation campaigns are also stirring up politically motivated violence through social media, particularly at times of political controversy. In 2019, there were just 6 conspiracy-theory based terrorist attacks. In 2020, the first year of the Covid pandemic, that number skyrocketed to 116 (Farrell, 2022). Those attacks mostly targeted public infrastructure (which some demagogues blamed for the outbreak of Covid (Langguth et al, 2023).

A lot of the responses to this new threat landscape are focused on having social media providers remove disinformation content as quickly as possible, which is subject to numerous recent regulations that are facilitated by in-depth technological research (McCabe, 2024). However, the role of law-enforcement agencies (LEAs) that do not have a mandate to detect, let alone remove, false allegations from the digital sphere, or elsewhere, in the fight against disinformation activities has often been overlooked.

Advancing LEAs' capabilities to rein in illegal disinformation activities and the ramifications thereof requires innovative technological solutions that mitigate the following challenges:

- Facilitate **investigations** by grasping the spread, origin and influence of disinformation campaigns on social media
- Perform **near real-time threat assessments**, so LEA personnel can be dispatched to areas of concern in due course
- Take proper **counter-measures** that stem the tide of disinformation campaigns causing social tensions, unrest and even violence

The Fake News Risk Mitigator (FERMI) project develops such innovative solutions and integrates those into a joint platform. More specifically, a spread analyser tool captures all re-tweets, quotes and replies to an initial disinformation message

on X. Accordingly, LEAs do not need to search such messages manually but get an overview of all exchanges involving the disinformation message at stake in a streamlined manner. Moreover, the spread analyser indicates the messages' origin by examining whether an account is likely to be human- or bot-operated, crucial to enabling LEAs to determine whether they can launch an investigation into a social media user or, alternatively, if said user has used a bot/numerous bots and remains to be identified. The spread analyser can distinguish between human- and bot-operated accounts with an accuracy of 83% and a weighted F1-Score of 82%. The influence of each social media user involved in the above-mentioned exchanges is rated, too, which can equip LEAs with further evidence to make their case in court, if charges are filed.

Influence of each user reveals which are particularly likely to be a catalyst for offline trouble, given their capacity to quickly reach a (relatively) huge audience. Monitoring such accounts can, therefore, advance in-depth threat assessments. Aside from that, such assessments rely on modules that capture the sentiment of all social media posts at stake (indicating the atmosphere in the disinformation community) and crime estimation together with privacy-preserving data protection tools that can estimate changes in the crime landscape (focusing on four crimes likely to be particularly influenced by extremist ideology, namely assault, destruction/damage/vandalism of property, disorderly conduct and larceny/theft) on a NUTS-2 level ideally over a 4-12 week time-frame without requiring LEAs to share highly sensitive training data with each other (thanks to the swarm learning framework).

Lastly, the necessity of counter-measures is analysed by grasping the likely impact of disinformation campaigns in terms of costs. Said impact is calculated by measuring how the estimated number of crimes presumably translates into the likelihood of crime occurrence leading to costs taking population size, amongst other things, into account. Aside from that, a given region's productivity at a certain time is calculated in view of politically motivated extremist crimes, which includes their ideological roots and nature. In the event said costs are categorised medium or higher the platform proposes counter-measures that are informed by intensive LEA feedback collected in a series of focus groups-like expert interviews.

Acknowledgements

The FERMI project is funded by the EU. I would like to thank my colleagues Michael Victor Lo Giudice and Joaquín García Gómez for their valuable comments and edits, all partners involved in developing the FERMI platform's models and tools and the entire FERMI consortium for their contributions to the project.

References

1. EUvsDisinfo. (2024). European elections. Retrieved from https://euvsdisinfo.eu/european-elections/.
2. Farrell, L. (2022). UMD Report: Conspiracy theories fueled more terror attacks in 2020. Retrieved from https://www.start.umd.edu/news/umd-report-conspiracy-theories-fueled-more-terror-attacks-2020.
3. Jones, I. and Comerford, M. (2023). Radical reinforcement: The January 6 attack and the methodology of hybridized extremism. Digital Dispatches. Retrieved from https://www.isdglobal.org/digital_dispatches/radical-reinforcement-the-january-6-attack-and-the-methodology-of-hybridized-extremism/
4. Langguth J., Filkuková P., Brenner S. et al. (2023). COVID-19 and 5G conspiracy theories: long term observation of a digital wildfire. International Journal of Data Science and Analytics, 15(3), 329-346.
5. McCabe, S.D., Ferrari, D., Green, J. et al. (2024). Post-January 6th deplatforming reduced the reach of misinformation on Twitter. Nature, 630, 132–140.

INHERIT:

INHibitors, Explosives and pRecursor InvesTigation

Hans Önnerud[1], Jonas Bengtsson[1], Stefan Ek[1]

[1] **Swedish Defence Research Agency,** Sweden

Keywords

Home-Made Explosives, HME, Precursors, Dilution, Inhibition, Markers, Detection, Forensics

Extended Abstract

The terrorism timeline consists of multiple phases, where all of those possess vulnerabilities that can be used to disrupt an attack. Due to the large diversity in precursors, there is no general approach yet that can be taken to keep a terrorist from using them to make explosives. INHERIT[1] is a security sensitive project that has addressed a multi-disciplined approach to intervene across multiple phases of the terrorism timeline. With a focus on explosive precursor chemicals, INHERIT used technologies directed towards thwarting the ability of terrorists to exploit these materials for production of explosives. Methodologies to render chemicals inert, more readily detectable and capable of yielding greater pre-forensic value have all been pursued. A collaboration between different partners that have developed these interventions have ensured a coordinated approach across the threat materials identified.

The EU precursor legislation[2] is an example of one step in the disruption of the timeline. This measure aims to restrict the availability of a precursor, either by a ban, a concentration limit, or through requested reporting of suspicious transaction to authorities. The use of dilution of a precursor, or reporting requirements of its purchase, allows for normal use for a consumer, while disrupting illicit application. Despite the present precursor restrictions, HMEs can be made from available consumer products. Therefore, the chemical and physical characteristics of the studied HMEs have been thoroughly assessed. The present availability of related materials has created an understanding on how to support law enforcement agencies.

Improvised explosive devices based on explosive peroxide compounds have become one of the preferred choices among terrorist organisations. INHERIT has worked on the development of inhibition (the adding of small amounts of additives to precursors) to obstruct the production of such explosives.

INHERIT has aimed to intervene across the terrorism timeline by the development of methods that contributes to that explosive precursors are more inert against misuse, easier to detect, and yield greater forensic value. It is fundamental to understand and follow current and emerging threats linked to HMEs, how they are synthesised, i.e. from which precursors they are produced in order to prevent misuse. Furthermore, the synthesised HMEs created opportunities to work on the development of other countermeasures such as detection and analysis of explosives.

INHERIT has also addressed precursors that are very difficult to be inhibited, such as fertiliser mixtures. For this topic, named markers and their detection, two types of commercially available techniques were chosen and assessed and they are Radio Frequency Identification tags (RFID) and Non-Linear Junction Detection (NLJD).

INHERIT has identified two non-regulated precursors that can be made into energetic materials. For one precursor, dilutions studies were performed in order to understand when the energetic material is mitigated. INHERIT has tested and assessed different scenarios concerning the chosen technologies for markers and their detection and also developed new methods for pre-blast forensics where e.g. novel sampling protocols is one highlighted feature of them.

Some of the results of the described topics (see Figure 1) will be presented to conclude the research activities that INHERIT has made over the project duration, to the extent possible considering the security sensitive topic.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021330 This article reflects only the authors' views and the Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains.

References

1. https://h2020-inherit.eu/
2. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32019R1148

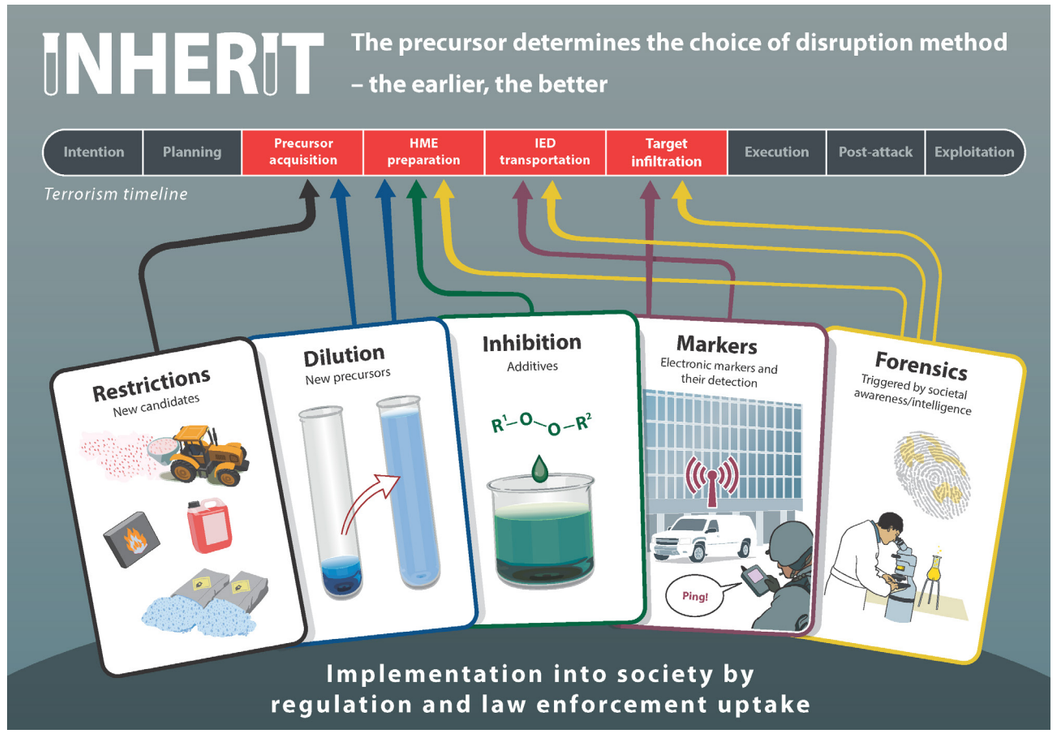


Figure 1: The concept of the INHERIT research methodology.

LAGO:

Laying the foundation for a trusted European FCT Research Data Ecosystem: the LAGO approach

Ernesto La Mattina[1], Valentina Mazzonello[1], Bernardo Pacheco[2], April Murray Cantwell[3], Axel Weißenfeld[4], Athanasios Psaltis[5], Christos Baloukas[6], Nikolaos Peppes[6], Badr El Mazaz[1], Valerio Scarfone[1], Salvatore Vicari[1], Vito Morreale[1]

[1] **Engineering Ingegneria Informatica S.p.A.**, Italy,

[2] **Instituto de Engenharia de Sistemas e Computadores Inovação**, Portugal,

[3] **Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research**, Sheffield Hallam University, United Kingdom,

[4] **Austrian Institute of Technology**, Austria,

[5] **Centre for Research and Technology Hellas**, Greece,

[6] **National Technical University of Athens**, Greece

Keywords

Research Data Ecosystem, Fostering FCT Research, Data Issue, Governance model, Reference Architecture

Extended Abstract

LAGO (**L**essen Data **A**ccess and **G**overnance **O**bstacles) project[1] aims to deliver the foundation for a trusted European FCT (Fight against Crime and Terrorism) **Research Data Ecosystem (RDE)** to address the so-called "Data Issue" in the FCT research landscape, i.e., the lack of domain-specific data in sufficient quality and quantity to enable appropriate training and testing of the developed methods, platforms and tools. LAGO is instrumental in identifying common barriers and subsequently providing the structural, governance and technical foundations to foster and innovate data-oriented research collaboration among EU Law Enforcement Agencies (LEAs), security practitioners, EU agencies, academic and industry researchers, policy makers and regulators.

To this end, LAGO has designed a comprehensive Reference Architecture for the FCT RDE for these actors to deposit, share and co-create data and tools for FCT research purposes based on common rules, protocols, standards and instruments in a trusted and secured environment. The envisaged Reference Architecture and accompanying governance framework are based on the design principles of the EU Data Strategy 2020-2025 that represents the inspiring pillars around which LAGO operates: security and trust (confidence in the identity and capability of participants), data sovereignty (data are subject to the laws of the country in which they are located), decentralisation (with no unique central repository, but data stored at source, and shared via semantic interoperability only when necessary), data quality (to ensure research data shared between participants are not corrupted, well-formatted and compliant with agreed formats), proportionality and risk (providing measures to assess risks of sharing data in particular contexts-requesting participants, purpose of use, etc.-and proportionality between the legitimacy of the sharing and the ethics, legal and privacy compliance), openness (in terms of rules, specification, and protocols to participate in data sharing and exchange), transparency (clarity on what happens to data), interoperability and portability (enabling the exchange of data through technical means and standard protocols), and ethics, legal and privacy compliance, especially focusing on FCT domains, where access to research data needs to consider EU regulations, national frameworks, ethics, privacy and data protection measures.

The proposed Reference Architecture consists in a decentralised data repository, which guarantees full control to data providers in terms of which data to make available, to whom, and under which conditions (i.e. licences and usage policies). Participants maintain their datasets stored on their premises and provide access to them through dedicated software component (called Connector), which implements the standards and protocols defined for the RDE (fulfilling the envisioned interoperability and portability principles), enabling access and sharing of research data in fully controlled way.

Participants can advertise their dataset on a dedicated Catalogue. To ensure data sovereignty, only metadata about datasets are published on the Catalogue, while data remain safely stored on participant premises. Metadata include information about not only the nature of the datasets, but also the usage policies and licences under which the dataset is made accessible by the data provider. To improve interoperability, LAGO has developed the DCAT-LAGO-AP vocabulary for the representation of metadata, which is an extension of the DCAT-AP profile (SEMIC community, 2024) for sharing information about Catalogues containing Datasets and Data Services descriptions in Europe. In addition to metadata foreseen by DCAT-AP, DCAT-LAGO-AP includes metadata for specifying the provenance of the dataset, societal implications, legal issues, ethical considerations, privacy issues and security aspects related to the dataset, purpose, intended use, known uses, avoided uses, bias, limitations and risks.

Any participant can search datasets through metadata stored on the Catalogue and request access to a dataset to the corresponding data provider. If a license was already specified for the requested dataset, the data consumer must accept the license terms for that dataset. Other types of data may require the establishment of a contract between the data provider and the data consumer, specifying the purposes, terms and conditions under which the data are shared, usage policies, and any advisable clause to safeguard the parties and avoid data misuse. Once the terms and conditions of the exchange are agreed, the dataset can be transferred from provider to consumer. All activities occurring in the RDE are proper logged on an Ethereum-based ledger, thus guaranteeing transparency of the data sharing processes.

Trust between participants is ensured through a dedicated accreditation procedure performed by a trusted authority, responsible of verifying trustworthiness of new participants. If approved, a participant is provided with credentials that certify it has been verified as trusted and thus can join the RDE. Those credentials can be later exchanged between participants, to enable mutual verification and prove trust.

The ultimate ambition of LAGO is to go beyond the creation of a common repository, to innovate the FCT data-oriented research sphere by creating the crucial foundations for the sustainable, safe and trusted creation, co-creation, sharing and maintenance of training and testing datasets for the FCT research domain. LAGO provides the EU FCT Research Community with a complete **Reference Implementation**

[1] https://lago-europe.eu/

of the RDE able to support the provision of research datasets, to enable their effective usage through data quality assessment and testing strategies and lawful governance procedures. The effectiveness of the LAGO Reference Implementation is going to be demonstrated in different concrete cross-project scenarios applied in different security fields. Finally, LAGO is defining a **Policy Roadmap** with consolidated rules, conditions and considerations for the actual deployment of the EU FCT RDE. This roadmap is being developed in close collaboration with all relevant stakeholders within the FCT domain to ensure the proposed solutions and recommendations are sustainable, practical, compliant, and effective in delivering an EU FCT RDE.

Acknowledgements

The work in this paper has received funding from the European Union under grant agreement No 101073951. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

1. SEMIC community. (2024, June 14). DCAT-AP 3.0. https://semiceu.github.io/DCAT-AP/releases/3.0.0/

LAGO:

Integrating Data Quality and Risk Assessment Methods for Enhancing Trust in FCT Research: A Holistic Approach for AI and Data Governance

Nikolaos Peppes[1], Christos Baloukas[1], Theodoros Alexakis[1], Emmanouil Daskalakis[1], Lazaros Papadopoulos[1], Dimitrios Soudris1, Evgenia Adamopoulou[1], Konstantinos Demestichas[2]

[1] **Institute of Communication and Computer Systems,** Greece,

[2] **Department of Agricultural Economics and Rural Development, Agricultural University of Athens,** Greece

Keywords

Data Quality Assessment, Risk Assessment, Data Governance, Data Quality Indicators, Risk Clarification, Decision Making

Extended Abstract

The paper presents a comprehensive approach to integrate data quality and risk assessment methods tailored to FCT (Fight against Crime and Terrorism) research, focusing on enhancing trust and governance in AI-driven data environments. By employing advanced tools and methodologies, this work addresses the critical need for reliable, unbiased, and secure datasets in FCT research. Key components include the Data Quality Assessment (DQA) tool, which evaluates data consistency, integrity, and bias, as well as the Risk Assessment framework, which identifies and mitigates potential legal, ethical, and security risks associated with data sharing. This combined approach offers a robust solution to enhance data quality and governance, ensuring the safe and effective use of high-risk AI systems in FCT contexts aligned with the objectives of the LAGO project.

Introduction

The increasing reliance on AI and machine learning in the fight against crime and terrorism (FCT) necessitates the use of high-quality and trustworthy datasets. However, the acquisition and use of such datasets are often hindered by several challenges, including data heterogeneity, lack of standardization, potential biases, and privacy concerns. To address these issues, the LAGO project has developed a set of innovative tools and methodologies designed to enhance data quality and facilitate risk assessment in data sharing within the FCT research community.

The Data Quality Assessment (DQA) tool provides a systematic approach to evaluating research data quality by focusing on key indicators such as consistency, integrity, completeness, and data aging. This tool supports researchers and data providers by identifying data quality issues, including missing values, data poisoning, and biases that could undermine the reliability of AI models. Additionally, the DQA tool incorporates advanced techniques like steganography and tampering detection to safeguard against adversarial attacks, thus enhancing the security and veracity of research data.

Complementing the DQA, the Risk Assessment framework addresses the broader challenges of data sharing by evaluating various risk dimensions, including legal, ethical, and technological

aspects. By assessing the likelihood and impact of these risks, the framework offers mitigation strategies that help data providers overcome barriers to sharing sensitive datasets. This twofold approach—enhancing data quality and managing risks—ensures that FCT research can proceed with greater confidence, fostering a more secure and ethically sound use of AI-driven data.

One of the fundamental challenges in FCT research is the inherent complexity of the datasets involved. Data generated in the FCT context is often sourced from diverse and fragmented origins, including law enforcement agencies, public safety systems, and private institutions. The heterogeneity of such data increases the risk of inconsistencies, making it difficult to ensure data quality without robust assessment mechanisms in place. Furthermore, AI-driven systems used in FCT applications can be prone to biases, either due to incomplete data or underlying social biases that are unintentionally encoded into the datasets. These biases can lead to skewed results, potentially exacerbating inequalities or undermining public trust in the research outcomes.

To combat these challenges, the LAGO project's tools focus on minimizing the introduction of biases and on ensuring that the data used for AI modeling is free from external influence or manipulation. By integrating these tools, researchers can identify and rectify data integrity issues early in the pipeline, ensuring that the AI systems deployed in FCT environments produce fair, accurate, and reliable results. The methodologies introduced by the LAGO project represent a significant advancement in the field of data governance, particularly within the context of high-risk AI applications in FCT research. By promoting a culture of trust and accountability in data sharing, the project aligns with broader efforts to develop ethical AI frameworks that ensure transparency and fairness in automated decision-making systems. In an era where AI technologies are increasingly being deployed in critical security and defense scenarios, the importance of maintaining high standards for data governance cannot be overstated.

Together, these methodologies contribute to the overall objectives of the LAGO project by promoting the safe and effective sharing of high-risk datasets. The integrated approach not only enhances the quality and security of research data but also addresses the growing concerns around data privacy and compliance in FCT research, paving the way for more reliable and impactful AI solutions. By implementing such a holistic approach, the LAGO project ensures that the ethical and technical challenges of using AI in FCT are carefully managed, fostering greater public trust in these systems.

Acknowledgements

The work in this paper has received funding from the European Union under grant agreement No 101073951. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ODYSSEUS:

Explosive precursor detection through innovative online and analytical approaches

Christopher Harman[1], Nikolaos Stylianou[2], Helen Gibson[1], Theodora Tsikrika[2], Babak Akhgar[1], Stefanos Vrochidis[2]

[1] **CENTRIC, Sheffield Hallam University,** UK

[2] **Information Technologies Institute, Centre for Research and Technology Hellas,** Thessaloniki, Greece

Keywords

Content Acquisition, Dataset Generation, Secure Data Management, Named Entity Recognition, Coreference Resolution, Disambiguation

Extended Abstract

ODYSSEUS aims to counter the development of homemade explosives through the detection of explosive precursors. The effective acquisition, analysis, storage, and auditing of data supports such detection processes. To this end, four main tools; Secure Data Management Serve and Audit, Synthetic Transaction Dataset Generator, Content Acquisition, and Multilingual Textual Content Analysis are developed each serving as a vital component for the operation of the complete ODYSSEUS system.

Secure Data Management Service and Audit

The Secure Data Management Service (SDMS) is a secure datastore that provides the central data storage solution for the whole ODYSSEUS platform where all components can store and retrieve data from. Secure REST APIs are employed to ensure that only authorised access is permitted.

The SDMS focuses on storing data via structured Json format to store textual content in an organised manner in one of three data types: Artefacts, Entities and Links. Artefacts are instances of data points, such as a given web page. Entities are tangible things such as places or people that can be referenced to. Links are created to connect and describe the link between two given artefacts. Support for a multimodal data format is also supported, enabling the function to store files such as documents and media within the SDMS.

An Audit tool is also integrated within the platform which records each interaction made with the SDMS into a blockchain for the intent of a verifiable chain of custody for digital evidence. Records who or what interacted with a given piece of data, and what type of interaction was performed, such as create, modify and delete, are stored.

Transaction Dataset Generator

The Transaction Dataset Generator creates a stream of synthetic transactions which were used for the training and demonstration purposes of AI suspicious transaction detection tools. The generator aims to create realistic data where there is a lack of available real-world labelled data is present. Multiple levels of the supply chain are implemented, following products from manufacturers to distributors to stores then onto the individuals.

The generator operated via an agent-based model simulation, creating malicious actors that aim to purchase the constituents of a homemade explosive recipe whilst employing activities with the intent to

disguise their activity. This was developed alongside input from LEAs to guide the methods used by the synthetic agents to closely relate to activities observed in real cases.

Variables and parameters used to generate the transactions are freely modifiable to finetune and modify the process to direct the generator, these include but are not limited to: Location of transactions, number of agents within the simulation, recipes and products targeted by agents and timescale of transactions.

While initially developed with the focus on the purchasing of products for HMEs, it may be employed in a wider variety of context with little required modification needed to begin accurately producing datasets where openly available examples are not present.

Content Acquisition and Extraction

The Content Acquisition tool is a series of components that automatically collect data from online sources for the use in discovering activity and information. A web crawler capable of targeting both the surface and dark web, social media crawlers targeted at Reddit and YouTube as well as a marketplace extractor are all employed within the ODYSSEUS platform aiming to carry out relevant activities by discovering discussions and products relating to HME recipes and precursors.

Data that is collected from online sources are processed by content extraction with the intent to clean the data before it reaches the analysis components of the system. Language detection is used to label the data to a language, and noise is reduced by removing unnecessary data such as HTML from webpages and retaining the main textual content.

Multilingual Textual Content Analysis

The Multilingual Textual Content Analysis tool is a collection of components which facilitate the conversion of unstructured content collected through the Content Acquisition tool into structured knowledge. This transformation ensures easy access to critical information pertaining to homemade explosives. Multilingualism is achieved through the accurate translation of collected content to English to enable advanced processing of the textual contents.

The analysis happens in three steps. An Information Extraction component is responsible for identifying and extracting entities and concepts of interest, trained on manually annotated datasets to fit our needs and augmented with external Knowledge Bases. Coreference Resolution is used to group all mentions of key information within the text, making it easier to follow specific pieces of information. Lastly, extracted information are being disambiguated, through linking the mentions of external knowledge bases offering detailed information about the contents identified.

Acknowledgements

ODYSSEUS is funded by the European Union's Horizon 2020 Research and Innovation Framework Programme under grant agreement no 101021857.

PERIVALLON:

Fighting Environmental Crime: the PERIVALLON use case for Illegal waste disposal detection

Eva Muñoz Navarro[1], Eduardo Villamor[1], Konstantinos Gkountakos[2], Theodora Tsikrika[2]

[1] **ETRA INVESTIGACIÓN Y DESARROLLO, S.A.,** Spain,

[2] **Information Technologies Institute, CERTH,** Greece

Keywords

Environmental Crime, Geospatial Intelligence, AI Multimodal Analytics, Intelligence Picture, Waste Disposal

Extended Abstract

Environmental crime is currently identified as one of the most critical organised crime threats faced by the EU and is undeniably on the rise. Fighting against it is particularly challenging due to the diversity of possible scenarios, including a wide range of items and substances illegally transported, smuggled and/or traded, intentionally dumped in soil or waters. Such forms of crime can be difficult to detect and to investigate by conventional means, highlighting the need for more sophisticated solutions enabling remote identification and evidence collection, as well as multimodal analysis and correlation of the information obtained. The EU-funded PERIVALLON project develops effective and efficient tools and solutions for detecting and preventing such types of criminal activities and for assessing their environmental impact, aiming at providing an improved and comprehensive intelligence picture of organised environmental crime.

PERIVALLON specifically tackles waste-related crimes as the top priority concern of practitioners. Intentional dumping of polluting substances, illegal disposal of (hazardous) waste, (cross-border) illegal trafficking of waste, and illegal trade of Hydrofluorocarbons (HFCs) are examples of criminal activities prioritised by the end-users (including Police Authorities and Border Guards). Therefore, the project is a user-driven project that will demonstrate its results through four transnational Pilot Use Cases (PUC) instantiated at 10 pilot demonstrations, involving one EU Agency, 4 Police Authorities (Italy, Greece, Sweden, and Moldova), 1 Border Guard (Romania), and 3 National and Regional Authorities (Belgium, Greece and Italy).

The first PUC to be demonstrated in PERIVALLON is PUC1 entitled "Illegal waste disposal detection". Waste disposal's multifaceted challenges have severe implications for environmental sustainability, economic stability, and social equality. The alarming increase in the scale of waste generation, the inefficiency of waste management systems, and the profitability of environmental crimes combine to create a complex, urgent problem requiring immediate, multi-layered solutions. In this context, PERIVALLON has developed a set of AI and analytical tools allowing the detection and identification of the exact location of illegal waste disposal sites. These tools include a geospatial intelligence detection tool suite, UAV detection for waste and land pollutants module, the optimised 3D terrain module, a Risk assessment for decision support module and the Environmental crime monitoring centre module, among others. Relevant data sets include satellite

imagery, UAV imagery, waste disposal sites and EWC-Stat[1] categories for investigation.

This paper describes the implementation of Pilot Use Case 1 "Illegal waste disposal detection" in PERIVALLON, focusing on the motivation, the scenario developed to demonstrate this PUC, and the first demonstration activities carried out in the pilot sites of Italy, Greece and Sweden, including the findings concerning the user experience evaluation and lessons learnt, to be further applied in the following PUC demonstrations.

Acknowledgements

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073952.

References

1. PERIVALLON D2.1 - Co-creation of use case scenarios, specification of user and security requirements

[1] European Waste Classification for statistical purposes

SAFEGUARD:

Safeguarding public spaces through intelligent threat detection tools

George Kalpakis[1], Chris Theodosiadis[1], Theodora Tsikrika[1], Stefanos Vrochidis[1]

[1] **Information Technologies Institute, Centre for Research and Technology Hellas,** Thessaloniki, Greece

Keywords

Protection of Public Spaces, Terrorism, AI, OSINT, LEA Operations

Extended Abstract

The recent terrorist attacks that have targeted open and easily accessible public areas in several European cities, including malls, crowded gathering areas, places of worship, and transportation infrastructures pose a challenge for Law Enforcement Agencies (LEAs) to provide effective countermeasure solutions for the protection of public spaces. Increasing pressure is put on governments and European authorities, given the rise of extremist activities perpetrated by organisations, groups, or radicalised individuals (known as lone wolfs) with an underlying political or ideological orientation, which severely impact citizens, disrupt the socioeconomic stability of modern societies, and undermine public confidence in national authorities. The recent terrorist attacks in Europe have also uncovered the extensive abuse of Surface, Deep, and Dark Web and social media services, used as cross-cutting enablers of terrorist activities, in terms of orchestrating operations and recruiting new members and perpetrators of future assaults [1]. In this context, it is important for LEAs to monitor suspicious behaviour in public spaces prior to and during large events of interest, leveraging advanced and targeted technologies aiming to correlate potentially criminal and/or terrorist activities (e.g., relevant information from social media, suspicious objects in a crowd, suspects etc.) in near real-time, in order to prevent and mitigate a potential threat.

Towards addressing these challenges, the SAFEGUARD[1] project (https://safeguard-project.eu/) aims at integrating, validating, and demonstrating a next-generation holistic suite of tools that significantly improves LEA capabilities to protect public spaces through the entire lifecycle of their operations, by investigating, detecting, assessing, preventing terrorist and extremist activities targeting public areas. The project leverages the outcomes of other successful EU-funded projects[2] and builds on top of a rich suite of intelligent threat detection tools developed in the context of these projects.

In particular, SAFEGUARD develops a powerful open-source intelligence platform gathering and analysing data from online media resources based on advanced Artificial Intelligence (AI) methods, including Web and social media crawling, multimodal analytics, visual analytics, and threat assessment, capable of monitoring and detecting threats targeting public areas, supporting pre-occurrence terrorism prediction and prevention. In addition, it is equipped with a Command & Control dashboard configured to monitor public areas of interest in (near) real-time during a LEA operation, leveraging the opportunities offered by modern technologies, such as

[1] The SAFEGUARD project full name is: "Safeguarding public spaces through intelligent threat detection tools".

autonomous robotic systems and IoT-enabled sensors. Unmanned Aerial Vehicles are employed to provide dynamic coverage of the protected public area, whereas IoT devices and sensors, including (but not limited to) fixed, mobile, or drone-carried cameras will contribute to acquiring better situational awareness. The multimodal data streams acquired by the IoT devices are utilised to ensure the visual monitoring and tracking, including object detection, activity recognition, and crowd analysis capabilities based on AI technologies. Intelligent threat assessment techniques are applied to support the provision of early warnings during a LEA operation, whereas the delivery of pertinent information and alerts to LEA officers will be actualised through the employment of user-friendly dashboards and Augmented Reality. Finally, SAFEGUARD is equipped with 3D-reconstructed and Virtual Reality-based simulations for sites of interest, including buildings, squares and other public areas relevant to LEA operations, in an accurate and visually convincing manner, so as to facilitate operational and tactical planning, and training. The SAFEGUARD solution is being developed in a user-driven manner based on the requirements of LEA personnel and domain experts and will be validated in a series of field tests and demonstrations based on bona-fide operational use cases with the active involvement of Greek and Bulgarian LEAs.

Acknowledgements

This project has received funding from the European Union and the Greek HOME Affairs Fund "Safety for All" 2021-2027.

References

1. Europol, T. S. European Union Terrorism Situation and Trend Report 2023 (Luxembourg: Publications Office of the European Union, 2023). https://data.europa.eu/doi/10.2813/370206, 52.

[2] S4AllCities with Grant Agreement No 883522, CONNEXIONs with Grant Agreement No 786731, CREST with Grant Agreement No 833464, PREVISION with Grant Agreement No 833115), and PRAETORIAN with Grant Agreement No 101021274

TENACITy:

Governance framework in travel Intelligence; the TENACITy holistic approach to crime prevention

Panos Karaivazoglou[1], Rodoula Makri[1], Chrysostomos Antoniou[2], George Boultadakis[2]

[1] **Institute of Communication and Computer Systems,** Greece,

[2] **European Dynamics Luxembourg SA,** Luxembourg

Keywords

Risk Governance, Travel Intelligence, LEAs, Crime Prevention, Passenger Information Unit (PIU)

Extended Abstract

Information systems with travel data are becoming an important decision-making tool for the safety and security of European citizens. However, implementation problems and inconsistencies are reported from the Europe's LEAs; incomplete or inaccurate data, missing datasets or irregular insertions into the information systems. Regulatory and "cultural" issues prevent Member States national units of exploiting all central EU functions available or even lead to different perceptions and methodologies on how their data management should be addressed (ECA, 2019). TENACITy addresses these challenges by offering to Security Authorities: a) Modern and effective tools for the use of passenger data, based on game changing digital technologies and an interoperable open architecture for the integration and analysis of multiple transactional, historical and behavioral data from various sources and b) Training and sensitization of LEAs' staff through setting up "living labs", hackathons and workshops for all involved stakeholders.

Above that, the main concept core is the provision of an overall implementation scheme for crime prevention through the **TENACITy's Travel Intelligence Governance Framework (TIGF)**. By this way, the project aims to tackle the main issues of travel intelligence usage through a holistic and systematic organizational approach and governance procedure, ensuring that the proposed digital technologies will effectively support the identification of the modus operandi of criminal and terrorism organizations. **TENACITy's TIGF** is a collaborative governance solution meant to address the different needs and interests as well as the different ways of thinking and acting of the relevant stakeholders (Governments, PIUs, practitioners, airline carriers, the public). The elicitation of TENACITy TIGF builds upon previous risk governance reporting (IRGC, 2017) and work (Heinimann & Hatield, 2017), expanding the relevant design to incorporate five distinct but interconnected processes, as depicted below:

- **Pre-assessment** which serves to illuminate diverse viewpoints regarding an issue, delineate the subjects for examination, and establish the foundation for evaluating and handling the issue at hand. It encompasses and details the range of issues that stakeholders and the broader community might link with a particular risk, alongside the opportunities it may present as well as current benchmarks, practices, and norms that could refine the focus on the risk in question and

how it ought to be approached.

- **Appraisal** extending beyond traditional risk analysis to include: a) a risk assessment of the relevant concrete, physical and quantifiable features to pinpoint the likelihood or range of possible adverse outcomes by examining the hazard, the exposure and susceptibility of the assets or values at stake and b) a concern assessment of the stakeholders' views and worries, involving a methodical examination of the relationships and perceived impacts that stakeholders link with a hazard, including its causes and effects.
- **Knowledge Characterization and Risk Evaluation** where the above outcomes are compared against specific criteria to determine the importance of the risk and prepare decisions. The generated knowledge is crucial for risk identification (as primarily simple, complex, uncertain, ambiguous, or often a mix) to determine the stakeholder participation in the governance process and in formulating strategies. An initial evaluation of a risk's acceptability (Acceptable, Tolerable, or Intolerable), incorporating tied perceptions and values (societal aspects, economic benefits and political factors), guides the demand for distinct approaches e.g. requiring extensive stakeholder involvement or longer-term risk governance efforts.
- **Management** being the systematic decision-making process which includes the creation, analysis, evaluation and selection of suitable management options, deciding on a specific strategy and its application under different future scenarios, and carrying out the chosen approach towards planning and executing actions aimed at avoiding, minimizing (through prevention, adaptation or mitigation), transferring or retaining risks.
- **Communication**, integral throughout all the previous stages, which involves the exchange of risk-related information among various groups, as scientists, regulators, industry, consumers, and the public. Effective, early communication is vital for successful risk governance being the platform for both risk assessors and managers as well as stakeholders and society to grasp the risk and its governance fostering a deliberate two-way dialogue.

Being defined as 5 interacting processes, TENACITy's TIGF can be adopted as a whole or just the desired parts can be inserted in existing procedures. Therefore, it functions as an umbrella covering all TENACITy's components being their integration and convergence; i) the **risk management framework**, as a scientific component, provides the core scientific knowledge of the appraisal and evaluation processes, ii) the **legal and regulatory framework** sets the context in the pre-assessment, but also affects all processes, imposing the restrictions and rules to be followed, iii) while **the open architecture** (technological component) is in fact part of the management process, providing the means to address and handle gaps identified by the other processes under a variety of scenarios and conditions. All are parts of the TIGF interacting with its processes, forming the TENACITy holistic governance solution advancing travel intelligence procedures.

Depending on the scenario at hand, the applied processes' implementation and evaluation may lead to obtain "framework blueprints", i.e. governance plans for travel intelligence usage customized to use cases realistic conditions. The TIGF collaborative aspect is essential as a direct consequence of the involvement of multiple actors belonging to various sectors, under different scopes and with diverse operational parameters. Thus, it provides new capabilities to **policy and decision makers** to test emerging changes, to shape new regulations or to define best practices and future policies improving the existing ones. Also, **practitioners** can advance the performance of the current procedures better organizing their activities.

Acknowledgements

TENACITy project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048.

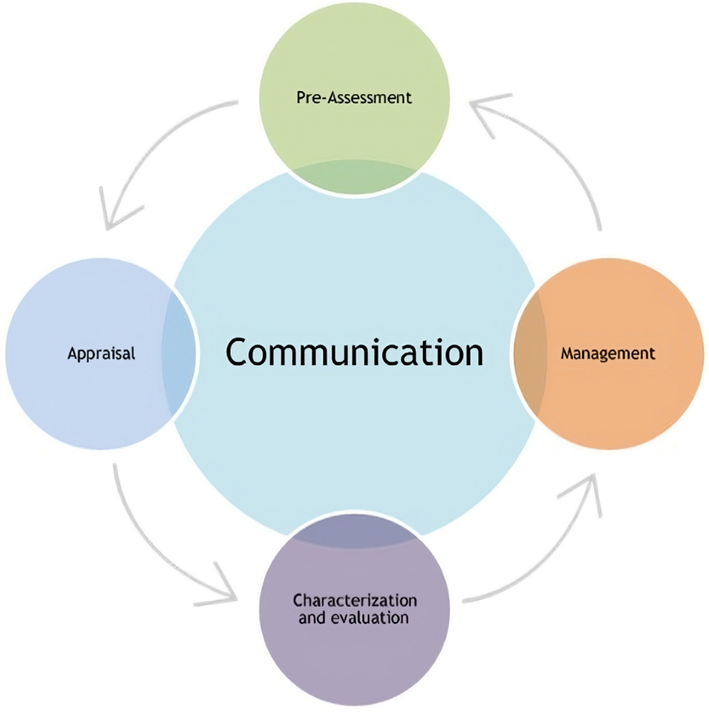


Figure 1: TIG Framework Structure

References

1. European Court of Auditors - ECA. (2019). EU Information Systems supporting border control – a strong tool, but more focus needed on timely and complete data, Special Report
2. Heinimann, H. R., & Hatield, K. (2017). Infrastructure Resilience Assessment, Management and Governance-State and Perspectives. Em Resilience and Risk-Methods and Application in Environment, Cyber and Social Domain (pp. 147-187). Springer.
3. IRGC. (2017). Introduction to the IRGC Risk Governance Framework, revised version. Lausanne: EPFL International Risk Governance Center. https://infoscience.epfl.ch/handle/20.500.14299/143682

TENACITy:
Anomaly Detection in Passenger Name Records

Neil Ireson[1], Muhammad Fadlian[1], Vita Lanfranchi[1]

[1]The University of Sheffield, UK

Keywords

Anomaly Detection, Border Security, PNR/API

Extended Abstract

In 2024 there will be approximately 9.5 billion global air passengers, with 43% (4.1 billion) of these being international passengers (ACI 2024). Such massive and increasing passenger volume creates the need for border management practices to adopt automated data processing and analytics to maintain fluid cross-border movements while upholding border security. To this end, Passenger Name Record (PNR) and Advance Passenger Information (API) are being employed in the identification of Subjects of Interest (SOI), i.e. known suspects and criminals, or unknown individuals who exhibit suspicious characteristics, associations or behaviours.

This paper presents a methodology to identify unknown (i.e. not already on a watchlist) potential SOI from anomalies in their PNR/API data, using statistical and cluster-based unsupervised machine learning techniques. A key part of the methodology is the feature engineering (or transformation) process that combines domain knowledge and data analysis to transform the raw PNR/API data into meaningful features that more accurately represent the domain problem. This process involves the encoding of the features into a numerical form that enables machine learning techniques to be employed in the modelling of the domain.

PNR/API data, which is provided by passengers and collected by carriers, includes information on travel itinerary, booking/ticket information, contact details, amount and means of payment, etc. There are various features within this data that can be used to raise suspicion, for example, if the flight was booked just before departure and paid for in cash (Price, 2012, Chapter 6, p. 251). While individual anomalies, such as this, are unlikely to be sufficient to label a passenger as a SOI, they can be used to filter the mass of passengers to focus on those most likely to require further investigation. In addition, the specific anomaly types and severity can be used to highlight the pertinent fields within the PNR/API data. This requires: i) normalised metrics to measure and compare the relative severity (or importance) of anomalies, ii) a method for combining anomaly values into a global PNR/API anomaly measure, and iii) the ability to provide explanations to allow a human assessment of the anomaly. To address these requirements two anomaly detection approaches have been implemented, statistical and clustering based.

The statistical based approach calculates univariant statistics for each feature based on whether the feature is numeric or categorical. For numeric features, kernel density estimation is used to detect if the distribution is unimodal, in which case a standard z-score is used to measure anomaly, or multimodal distributions (for example with stay length, which tends to be either a few days, week or fortnight), in which case the distribution is split into multiple normal distributions using Gaussian Mixture Models and the anomaly measure calculated by z-score aggregation. For categorical features, anomaly is measured by the marginal relative frequency (i.e., the number of occurrences of category values). Where features are constructed from multiple categorical variables (e.g. origin and destination airports) conditional frequencies are used, which considers the marginal and joint (i.e. combination) frequency of categories. Global PNR/API anomaly is an aggregation of the individual feature anomaly measures.

For clustering it is first necessary to determine the distance between the instances (i.e. PNR/API) to be clustered. This is done using the Manhattan distance for numerical features and Jaccard distance for categorical features (these are first one-hot encoded). The instances are then clustered using a density-based clustering algorithm (DBSCAN), that segregates instances into high-density regions separated by regions of low density. The anomaly is then determined using a Cluster-Based Local Outlier Factor (CBLOF) approach, where anomaly is measured by size and degree of isolation of the nearest cluster to an instance.

The anomaly detection approach has been evaluated in a pilot study involving analysts involved in border management.

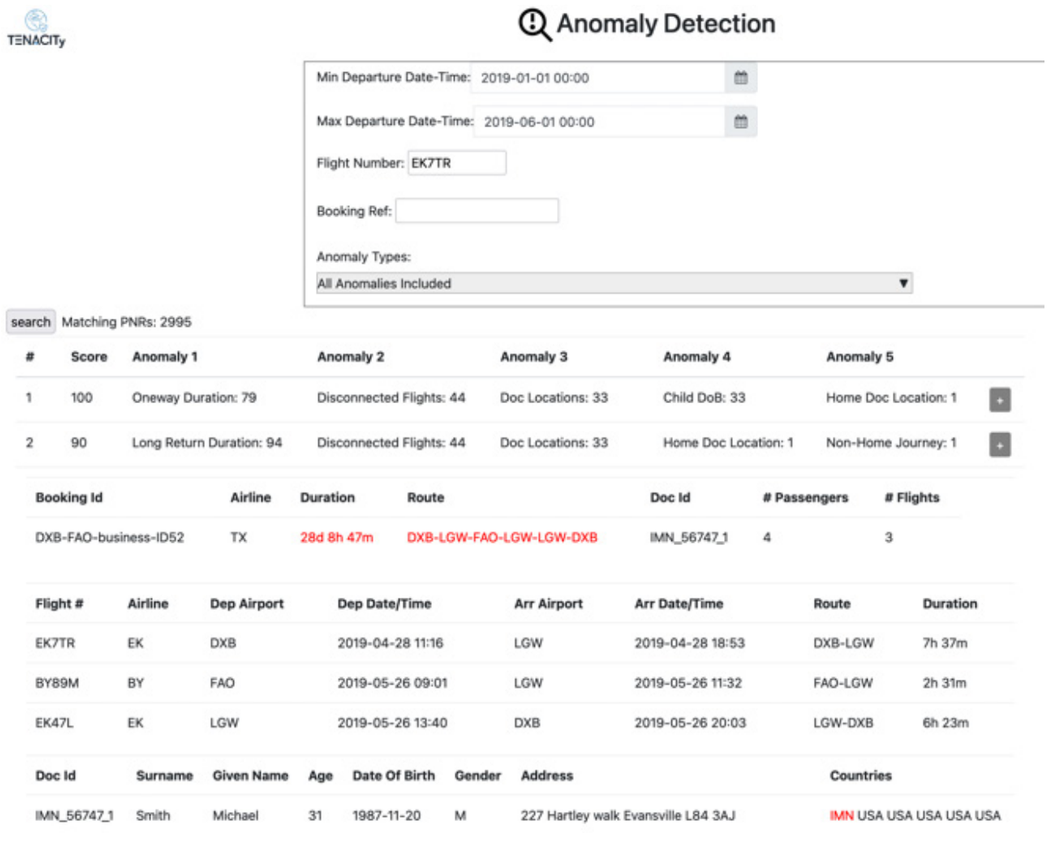


Figure 1: Anomaly detection user interface

The study used a synthetically generated PNR/API data set, the analysts searched for a set of PNR/API of interest (i.e. from a given flight or airport) and the anomaly measures were used to sort the search results. The results are then presented in a user interface (Figure 1), with the potential anomalies for each PNR/API highlighted for assessment by an analyst, in order to determine whether further investigation is warranted.

Currently only the statistical approach has been evaluated, as the explanation for the feature and global anomaly measures are more transparent and thus amenable to human interpretation and assessment. However, the clustering approach offers a potential advantage as it inherently considers all feature interactions when determining global anomaly. Future work will: i) examine methods to provide clustering explanation, e.g. by presentation of the differences between the instance, nearest cluster centroid and nearest large cluster centroid features, and ii) perform comparative evaluation between the statistical and clustering anomaly detection approaches.

Acknowledgements

This work has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101074048

References

1. ACI (2024). Advisory bulletins 18 Sep 2024 [Accessed: 2024-09-23]. https://aci.aero/2024/09/18/the-trusted-source-for-air-travel-demand-updates-2/
2. Price, J. (2012). Practical aviation security: predicting and preventing future threats. Butterworth-Heinemann.

TENSOR:

Reliable biomeTric tEchNologies to asSist Police authorities in cOmbating terrorism and oRganized crime

Eleni Veroni[1], Spyridon Evangelatos[1], Katerina Kyriakou[2,3], Apostolos Apostolaras[2,3], Thanasis Korakis[2,3]

[1] **Research & Innovation Development Department**, Netcompany-Intrasoft S.A., Luxembourg,

[2] **Department of Electrical and Computer Engineering**, University of Thessaly, Greece,

[3] **Centre for Research & Technology**, Hellas, Greece

Keywords

Multimodal Biometric Identification, Behavioural Biometrics, Biometrics Dataspace, Digital Forensics, Cross-Border Data Exchange, Generative AI

Extended Abstract

Biometrics address a longstanding concern to prove one's identity, irrefutably, by using what makes a person unique. Over the past few years, biometrics have transitioned from a novel technology to being an essential part of daily life, as more and more people leverage biometric authentication techniques to gain access in devices (mobile phones) and services (e-banking). Today, biometric identification is being combined with other advanced technologies such as behavioural detection, emotion recognition, and AI to serve an array of purposes, including healthcare, law enforcement, and border control.

In the law enforcement domain, the undisputable power of biometrics is being fully harnessed by Police Authorities and forensic investigators who have been relying since the 1980s on the Automated Fingerprint Identification Systems (AFIS) to tackle global terrorism, criminality, and illegal migration. However, matching the evidence-often smudged, incomplete, or deposited on top of other markings - with complete prints on file in AFIS databases remains a challenging task. To address this, TENSOR goes beyond traditional fingerprint-based identification by integrating multiple modern biometric modalities, including facial and voice recognition, with emerging behavioural biometrics like gait analysis and keystroke dynamics. Advanced AI models are leveraged by TENSOR to produce court-proof evidence.

TENSOR is driven by three core objectives, each translated into a distinct and real-world pilot use case:

(1) The first use case **aims at evidence collection through intelligence derived from correlated physiological and behavioural biometrics** based on CCTV footage. Lawful evidence derived from CCTVs (face, gait, voice) and contactless fingerprints scanners, are fused towards accurate and multimodal identification and criminal identity verification. TENSOR proposes a dynamic fusion mechanism combining multiple biometric traits for suspect identification. The solution integrates a suite of biometric identification technologies to extract actionable intelligence, leveraging data collected from crime scenes. The scope of data collection may vary depending on available sources. For instance, within areas covered by CCTV surveillance, modern physiological and behavioural biometric technologies can analyse footage to conduct facial and gait

recognition on suspects. This process also provides insights into additional features of the suspect crucial to investigations, such as clothing details, brand logos, the use of facial coverings, glasses, as well as identifying scars and tattoos. Voice recognition can further aid investigations when audio recordings are available, revealing details about the suspect's identity and spoken language. These biometric traits can then be used to deduce soft biometric attributes such as gender, age, height, race, and ethnicity. Each biometric identification technology produces individual biometric similarity scores generated by a biometric-based identification system, such as facial recognition or fingerprint matching. These scores signify a potential correlation between the biometric sample under analysis and a stored reference sample within a suspect database (e.g., AFIS), after assessing the degree of similarity between the two samples. TENSOR fuses the produced matching scores considering a predefined biometric taxonomy used for weight assignment through a weighted average formula which dynamically assigns varying weights based on the number and reliability of the analysed biometric traits and the confidence of the produced results, delivering a set of recommendations for the identities of the potential suspects.

Moreover, TENSOR offers an AI-powered Digital Assistant that leverages an offline large language model (LLM) to enhance and facilitate the investigative processes, serving as a valuable tool for Law Enforcement Agencies (LEAs) and Forensics Institutes. Various data inputs are integrated to provide enriched outputs in natural language. The process begins with the pre-processing of incoming biometric data to ensure accuracy and proper formatting. The data include the output of the Biometric Data Fusion software solution, with recommendations about suspects based on the produced biometric matching scores. The data are prepared for input into the LLM through prompt engineering, which involved creating queries that guide the LLM in generating relevant insights based on said data. The LLM processes these prompts to produce outputs that range from incident narration to information on investigation aspects and the produced results, delivered in a communicative form via a user interface (UI) communication endpoint. This solution acts as a digital assistant, offering interactive content and vital information in natural language, aiding the LEAs and increasing the efficiency of the investigation and reporting processes. It should be noted that the solution ensures compliance with the European Union's AI Act and guidelines for responsible AI usage.

(2) The second use case **aims at the utilization of digital forensic extensions for identifying the owner of an orphan mobile device**, often seized during police raids on criminal hideouts, by analysing behavioural data collected from these devices. As organized crime is increasingly planned, executed, and concealed online, there is an urgent need for access to digital evidence that can aid in identifying criminals through data stored on personal mobile devices such as smartphones, tablets, and laptops. These devices often hold a wealth of information-text inputs, GPS data, photos, videos, transaction records, and other behavioural traces-that can help reveal connections, establish timelines, and identify individuals involved in criminal activities, creating a crucial link between the crime, the perpetrators, and their victims.

To bypass the built-in security features of these devices, which are often equipped with hardware-based encryption (embedded Secure Elements), TENSOR proposes a set of methodologies to decrypt the device's file system. Once decrypted, an exploratory analysis of contextual (application-related) and behavioural data is performed to derive the behavioural profile of the device owner. This analysis can generate additional intelligence, such as the user's previous locations (inferred from images and GPS data), spending patterns, and other relevant insights that assist forensic investigators. Moreover, information can be extracted from popular apps, including messaging platforms, through the retrieval of input text. These text inputs offer further intelligence on the device owner, including sentiment, education level, languages spoken, emotional state, and attention to detail, providing valuable context for forensic practitioners.

(3) In the third use case, TENSOR **aims at implementing the first Biometrics Data Space ecosystem for sovereign and trustworthy cross-border data exchange.** As digital biometric technologies become more prevalent for enhancing identification and identity verification processes, concerns around privacy, ethics, and the need to comply with EU data protection regulations are growing. TENSOR introduces the concept of a Biometrics Data Space, a secure ecosystem built on Data Spaces technology, designed to facilitate the safe sharing and exchange of biometric data in cross-border scenarios where international cooperation among foreign Law Enforcement Agencies (LEAs) and forensic agencies from different countries is required. The goal is to support the reliable identification of suspects in a secure and trustworthy ecosystem without disclosing any personal sensitive information. The proposed framework incorporates Privacy Enhancing Technologies (PETs), such as homomorphic encryption, to mitigate data protection issues. Additionally, large-scale data indexing is used to quickly and efficiently compare facial images of suspects with those stored remotely, ensuring no personal information is revealed during the search and matching process. Furthermore, the system includes automated access rights control through Blockchain Smart Contracts, integrated within the Biometrics Data Space framework where data owners (e.g., any national forensic agency that maintains a list of suspects identified by their biometric data) define the data usage rules for the biometric data that is to be exchanged. Those rules are imposed and respected by the data consumers (e.g., forensic agencies that aim to identify a suspect in a database hosted by a foreign country agency).

Notwithstanding the importance of exchanging data in cross-border settings for criminal identification and case resolution, protecting and safeguarding personal data is of extreme importance to ensure that no sensitive information is disclosed and data protection rules are respected. Moreover, differences in national and international legislation for biometric data sharing create barriers and increase the complexity of the investigation process. The ultimate goal of TENSOR for creating the first biometric dataspace is to offer a trustworthy ecosystem for LEAs and forensic agencies, that guarantees enhanced biometric data protection and biometric data sharing can be regulated by strict data usage policies for sovereign data usage and control.

Acknowledgements

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101073920. This article reflects only the authors' views and the European Commission is not responsible for any use that may be made of the information it contains.

TESSERA:

Towards the datasets for the European Security Data Space for Innovation

George Kalpakis[1], Taxiarchis Skouras[1], Theodora Tsikrika[1], Stefanos Vrochidis[1]

[1] **Information Technologies Institute, Centre for Research and Technology Hellas,** Thessaloniki, Greece

Keywords

Datasets, Data Models, European Security Data Space for Innovation, AI, National Components, Stakeholders' Involvement

Extended Abstract

Digital technologies have transformed all sectors of human activity, including the security domain. Modern digital technologies and in particular those fuelled by data-driven innovation, such as Artificial Intelligence (AI), provide law enforcement with new opportunities and enhanced operational capabilities to tackle criminal activities taking place both in the online and offline worlds, as well as in their cyber-physical convergence [1]. To this end, the availability, accessibility, interoperability, and (re-)usability of high quality trusted large-scale data from multiple heterogeneous sources is of paramount importance for training and validating data-driven tools and algorithms that can equip Law Enforcement Agencies (LEAs) with valuable information and insights helping them make critical decisions and fight crime in a more efficient and effective manner [2]. At the same time, ensuring that the data used for the development of disruptive technologies in the security domain are in full compliance with applicable data protection legislation and the Charter of Fundamental Rights is equally essential [3]. Moreover, avoiding systematic bias against any ethnicity, gender, nationality, or other social categories is fundamental in order to establish fairness and impartiality.

To address these challenges, the European Security Data Space for Innovation (EU SDSI) has been recognised as the cornerstone for implementing the European Data Strategy [4] in the security domain, within the context of the Data Spaces flagship initiative of the European Commission [5] aiming at the data sovereignty of Europe, while having as ultimate goal to increase trust in the use of Artificial Intelligence by Law Enforcement. The EU SDSI aims to enable the more effective and efficient fight against crime by providing a facility through which LEAs benefit from higher quantity and quality data that can be used for innovation purposes. From the technical point of view, the implementation of this facility requires the incremental development of a secure and energy-efficient cloud federation infrastructure consisting of national and central components. Equally important is the comprehensive understanding of the security-oriented dataset landscape and the definition of relevant standards permitting the production of interoperable and shareable datasets for training and validating tools for innovation purposes.

In this context, the TESSERA[1] project (https://tessera-project.eu/) aims to conduct the preparatory work for the creation of high-quality large-scale trusted and shareable datasets based on identified operational use cases, thus supporting the European Security Data Space for Innovation. Particular focus will be given on analysing and defining the requirements ensuring the interoperability and shareability of heterogeneous datasets, whilst considering their compliance to privacy preservation and protection of fundamental human rights. TESSERA also aims to specify the low-level architecture of the data-related national components of the European Security Data Space, including requirements related to user management, data access, and exchange, whilst also considering their interconnectivity and deployment in the federated architecture of the EU SDSI.

TESSERA builds upon and complements past and ongoing initiatives, including relevant initiatives by EU Agencies (such as Europol and eu-LISA), relevant EU associations (e.g., EACTDA), and EU-funded projects with relevant outcomes, while also fostering the engagement with and involvement of such stakeholders. To achieve its objectives, TESSERA will organize technical workshops that will facilitate the delivery of a report documenting the outcomes of the project. With a consortium of seven partners, including law enforcement, research and industry partners with strong experience and expertise in the security domain and AI technologies, as well as experts on legal and ethical issues, TESSERA combines a wide expertise and delivers a strong representation of the challenges and requirements to meet its objectives.

[1]The TESSERA project full name is: "Towards the datasets for the European Security Data Space for Innovation".

Acknowledgements

This project has received funding from the European Security Funds under the topic ISF-2021-TF1-AG-DATA from the European Commission, Directorate-General for Migration and Home Affairs (DG HOME) - Grant Agreement No 101145802. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

1. Raaijmakers, S. (2019). Artificial intelligence for law enforcement: challenges and opportunities. IEEE security & privacy, 17(5), 74-77
2. Kusak, M. (2022, October). Quality of data sets that feed AI and big data applications for law enforcement. In ERA Forum (Vol. 23, No. 2, pp. 209-219). Berlin/Heidelberg: Springer Berlin Heidelberg.
3. Zhou, J., & Chen, F. (2023). AI ethics: From principles to practice. AI & SOCIETY, 38(6), 2693-2703.
4. EU Commission (2020). A European strategy for data.
5. European Commission. (2022). Commission Staff Working Document on Common European Data Spaces.

VANGUARD:

Early Detection and Response to Human Trafficking through Societal Analysis and Cutting-Edge Technology Solutions: The VANGUARD project

Theodora Tsikrika[1], Despoina Chatzakou[1], Theoni Spathi[1], Theodoros Semertzidis[1], Mascha Koerner[2], Carlotta Carbone[3], Krzysztof Mierzejewski[4], Donatella Casaburo[5], Christos Varsamis[6], Alexandros Rammos[7], Javier Ruiperez[8], Sara Diez Minguez[9], Philip Schneider[10], André Alegria[11], Vasileios Georgiadis[12]

[1] **Centre for Research and Technology Hellas,** Greece,

[2] **Gemeinsam gegen Menschenhandel e.V.,** Germany,

[3] **Università Cattolica del Sacro Cuore,** Italy,

[4] **Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego,** Poland,

[5] **Katholieke Universiteit Leuven,** Belgium,

[6] **Center for Security Studies,** Greece,

[7] **Institute of Communication & Computer Systems,** Greece,

[8] **Fundación EuroÁrabe de Altos Estudios,** Spain,

[9] **Atos IT Solutions and Services Iberia, Spain,**

[10] **Hochschule für den öffentlichen Dienst in Bayern,** Germany,

[11] **Ministério da Justiça,** Portugal,

[12] **Hellenic Police,** Greece

Keywords

Trafficking in Human Beings, Intelligence picture, Artificial Intelligence, Serious games, Awareness raising

Extended Abstract

Trafficking in Human Beings (THB) is a serious transnational organised crime with global ramifications, posing significant threat to international security, while violating fundamental human rights. It manifests in various forms, including trafficking for sexual and labour exploitation, forced begging, organ removal, forced marriages, and other forms of forced criminality. Reports from UNODC (2020) [1], SOCTA (2021) [2], and GRETA (2023) [3] indicate that 80% of detected criminal networks are involved in THB alongside other illicit activities. Perpetrators of THB take full advantage not only of societal and geopolitical situations, but also of technology, by integrating it into their business model at every stage of the process, with their activities increasingly taking place in the online domain. In particular, their operations, including recruitment, advertising, and exploitation, have largely shifted online, especially on social media and gaming platforms. Despite this shift, THB continues unabated in the physical world, with several EU countries serving as origin, transit, and/or destination countries, underscoring the need for effective measures to address THB also at their borders. The tripling of the number of identified victims between 2008 and 2019 underscores the urgent need to intensify efforts to combat the phenomenon more effectively.

The three-year EU-funded VANGUARD project aims to strengthen research and innovation efforts at the nexus of advanced technological solutions of sensing, analysing, understanding, awareness raising, and training to disrupt the trafficking chain at an early stage. In particular, VANGUARD aims to address the societal dimensions of (cross-border) THB-related criminal activities and the trafficking chain, through both desktop and empirical research (including interviews with THB experts, victims, and perpetrators), providing useful insights into the scale of THB at EU and global levels, the profiles of the actors involved, and the modus operandi at different THB stages, seeking to primarily untangle the complex dynamics of sex trafficking, labour trafficking, and forced criminality.

The capabilities of end users, including Police and Border Guard Authorities, to more effectively tackle such criminal activities will be enhanced through the development and provision of modular and trustworthy suite of tools for detecting, identifying, investigating, and preventing online-facilitated THB activities and THB-related activities at (border) checkpoints. The latest advancements of Artificial Intelligence (AI) in computer vision and multimodal analytics will be utilised to enable effective and efficient monitoring and analysis of online multilingual and multimedia content, as well as the processing and analysis of multimodal streams (e.g. video streams from surveillance cameras and thermal cameras streams), and remote sensing using fixed or movable terahertz (THz) devices.

Capacity building and training will be facilitated through both Virtual Reality (VR)-based serious games and synchronous and/or asynchronous learning methodologies tailored to practitioners' actual needs, addressing both societal and technological dimensions. To enhance knowledge exchange and information dissemination among relevant stakeholders, such as security practitioners on the one hand, but also non-governmental and civil society organisations (NGOs/CSOs), THB survivors, and the general public, a knowledge sharing and collaboration platform will be developed and delivered. Additionally, innovative awareness raising campaigns, both in the online and physical worlds, will be conducted, including an online game aimed at raising THB awareness among young people, along with additional informative material. Monitoring legal, ethical, and privacy aspects-including the analysis, definition, and oversight of personal data, fundamental rights, and privacy considerations-will be at the heart of all project activities involving the deployment, usage, and impact of the designed AI technologies.

Overall, VANGUARD will be validated in field tests and demonstrations in three operational use cases. Extensive training, hands-on experience, joint exercises, and training material will promote the adoption of VANGUARD tools and technologies. With a consortium comprising seven Police and Border Guard Authorities, one Police Academy, eight research/academic institutions, four industry partners (including two SMEs), and two Non-Governmental Organisations (NGOs)/Civil Society Organisations (CSOs) from 12 countries, VANGUARD provides robust representation of the challenges, requirements, and tools to achieve its objectives.

Acknowledgements

Co-funded by the European Union

Funded by the European Union – Research and Innovation Framework Programme, under grant agreement No 101121282. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or

the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

References

1. UNODC (2020), 2020. Global Report on Trafficking in Persons 2020, United Nations publication, Sales No. E.20.IV.3.
2. EUROPOL (2021), European Union Serious and Organised Crime Threat Assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, SOCTA 2021.
3. Council of EUROPE (2023), 13th GENERAL REPORT, GRETA Group of Experts on Action against Trafficking in Human Beings, GRETA 2023.

02. Civil Protection and Disaster-Resilient Societies

SILVANUS:

Empowering citizens to support prevention and preparedness in the wildfire management cycle

Youla Karavidopoulou[1], Iosif Vourvachis[1], Alexandros Giordanis[1], Dimitrios Iliadis[1]

[1] **Hellenic Rescue Team** (Greece)

Keywords

Wildfire Management, Raising Citizen Awareness, Citizen Engagement, Training, Prevention and Preparedness

Extended Abstract

SILVANUS, a Horizon 2020 Green Deal funded project, delivers a climate resilient forest management platform. This innovative technological platform provides the tools to prevent and combat wildfires, by offering decision-making support in the Prevention and Preparedness (Phase A), Detection and Response (Phase B), and Restoration and Adaptation (Phase C) phases of the wildfire management cycle while raising the human, environment and economy resilience to wildfires. The project's technological solutions are currently being tested and validated on the field through a 2nd cycle of pilot demonstrations across Europe and internationally. The pilot demonstrations bring together stakeholders represented by forest management authorities, public administration bodies, and fire fighters.

The project follows a holistic approach engaging stakeholders relevant to wildfire management through a participatory process, ultimately assisting authorities to efficiently monitor forest resources, evaluate biodiversity, generate accurate fire risk indicators and promote safety regulations among local communities. The novelty of SILVANUS lies in the development and integration of advanced semantic technologies to systematically formalise the knowledge of forest administration and resource utilisation.

More than 20 user products have been developed and are being integrated in the SILVANUS platform, ranging from training tools, mobile applications, to fire spread forecast and evacuation route planning. A **citizen engagement program** for preventing wildfires is underway, engaging citizens, towards improved awareness about fires, related risks, as well as prevention and safety measures to establish and nurture social and cultural behaviours and practices that lead to reduced fire hazards caused by human negligence or actions. A **citizen engagement mobile application** has been developed, serving as a fire management app targeted to citizens as the main users offering guidelines, practical tips, quizzes, and authorities/firefighters as the administrators. The primary objective of the app is to keep citizens informed, safe, and connected to emergency responders, covering all 3 phases of the SILVANUS project by being a comprehensive tool to assist citizens in preparing for, responding to, and recovering from fire incidents. It serves as an important channel for citizens to increase their awareness regarding wildfires and their impact as well as engage them in fire-prevention and rehabilitation actions.

In addition to the pilot demonstrations and the citizen engagement mobile application, a series of Prevention and Preparedness (Phase A) activities have been implemented and are currently being carried out in Thessaloniki by HRT. Activities such as seminars, webinars, interactive workshops, and live demonstrations have already been hosted by HRT to engage and empower the general public, equipping them with adequate knowledge for prevention and preparedness of wildfires, as well as engaging them in the development of the project's application.

Acknowledgements

The SILVANUS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 101037247. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the EC.

SILVANUS:

Innovative Machine Learning Models for Predicting the Severity of Forest Wildfires – Selected Case Studies

Dimitrios Sykas[1], Dimitrios Zografakis[1], Konstantinos Demestichas[1]

[1] **Agricultural University of Athens,** Greece

Keywords

Forest Fires, Deep Learning, Machine Learning models, Sentinel-1/Sentinel-2 Satellite Data, Fire Size and Shape Prediction

Extended Abstract

Many European countries frequently face the challenge of wildfires, with impacts that range from devastating environmental damage to significant human losses. Accurate prediction of wildfire severity remains a crucial challenge for both authorities and civil protection agencies, who must deploy resources efficiently and minimize risks to life and property. In this extended abstract, we present a comparative study of state-of-the-art deep learning models applied to predicting the size and spread of wildfires across a representative set of countries, including France, Germany, Greece, Italy, and Spain. Our work is based on the EO4WildFires dataset, developed as part of the EU Green Deal project SILVANUS, which supports integrated wildfire management.

The EO4WildFires dataset offers a comprehensive set of correlated satellite and meteorological data for the analysis and prediction of wildfire severity. It incorporates high-resolution imagery from Sentinel-1 and Sentinel-2, both of which provide critical multi-spectral data across a range of bands. These satellite systems capture essential spatial and temporal patterns, while the integration of meteorological data – including temperature, humidity, wind speed, and atmospheric moisture - further refines the models' predictive capacity. The dataset also includes a rich historical archive covering various regions across the European Union and neighboring countries over different time periods, making it a powerful tool for training and validating machine learning models in a diverse array of geographic and climatic conditions.

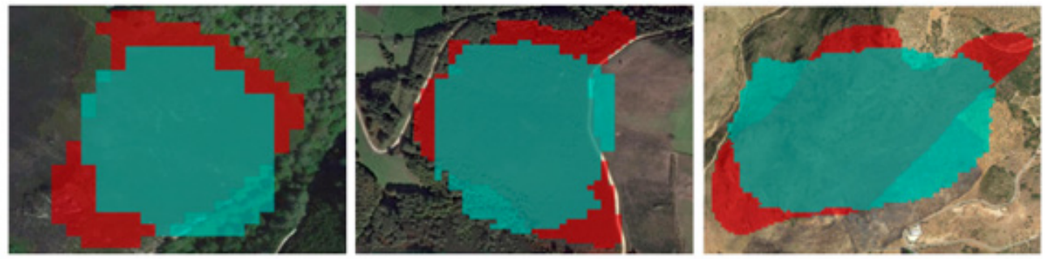
In this study, we developed machine learning models by leveraging the multi-parameter data provided by the EO4WildFires dataset. This includes satellite imagery from the Sentinel-1 and Sentinel-2 systems, combined with relevant meteorological data. The research focuses on two leading deep learning techniques: convolutional neural networks (CNNs) and visual transformer technologies, which are well-suited for processing large-scale visual and time-series data. Our aim was to evaluate these models' effectiveness in generating accurate predictions of wildfire spread, with an emphasis on identifying the architectures that offer the highest reliability for operational use.

Our experimental framework focused on assessing key performance metrics such as accuracy, sensitivity, and precision, specifically in predicting wildfire size (burned area) and shape (fire boundary contours). To facilitate a robust comparison, we developed a suite of metrics that measure the effectiveness of different model architectures, thereby enabling the selection of the most appropriate models for real-world applications in forest fire management.

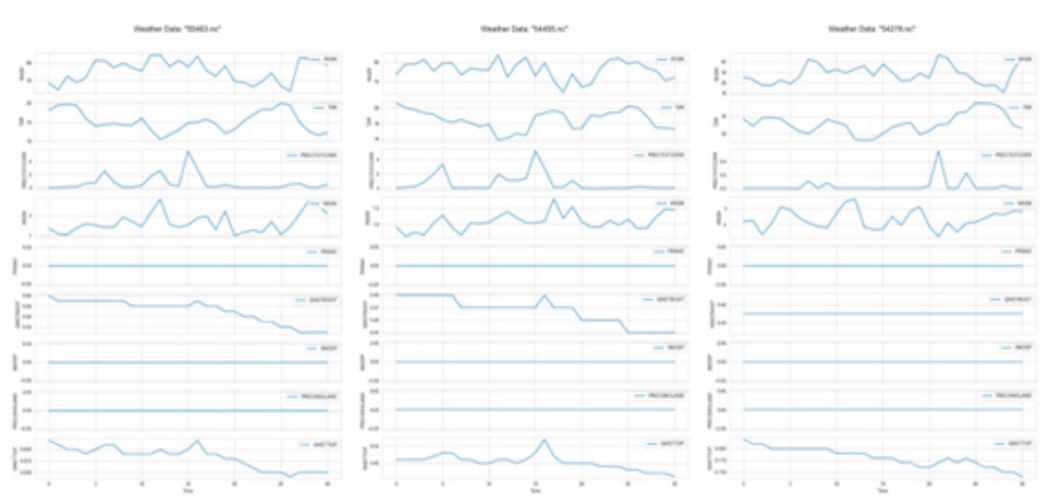
The results, part of which are illustrated in Figure 1, demonstrate the substantial potential of modern machine learning models in predicting wildfire severity. Both CNNs and visual transformer models achieved high accuracy in forecasting the affected areas, providing critical early warnings about the potential intensity and spatial progression of fires. The following key metrics were employed to evaluate model performance:

- F1 Score: Balances precision and recall, offering a comprehensive measure of overall model accuracy.
- Intersection over Union (IoU): Measures the overlap between predicted and actual burned areas, offering a robust metric for spatial accuracy.
- Average Prediction Deviation (aPD): Calculates the mean discrepancy between predicted and actual burned areas, reflecting the precision of the models in estimating wildfire impacts.

The integration of satellite imagery and meteorological data substantially improved the predictive capabilities of the models, while the ongoing refinement of the underlying algorithms promises



(a) Predicted (cyan) vs Ground truth (red).



(b) 30 days past meteorological time series variables.

Figure 1: Selected Examples – Case Studies

even greater accuracy and operational relevance in the future. The findings from this research have significant implications for enhancing wildfire prevention and mitigation strategies. Moreover, these advancements contribute to improved disaster management protocols, supporting both the safety of citizens and the protection of critical ecosystems in the face of increasingly frequent and severe wildfires.

This work provides valuable insights into the application of cutting-edge Artificial Intelligence (AI) technologies within integrated fire management systems, highlighting their potential to bolster preparedness and response efforts in regions prone to wildfire risk.

Acknowledgements

This study has been conducted in the framework of the SILVANUS project. This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 101037247. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

SYNERGISE:

SYNERGISE- increased safety and efficiency of first responder operations

Anastasios Dimou[1], Tiina Ristmae[2], Melanie Carevic-Neri[3]

[1] **CERTH**, Greece,

[2] **THW**, Germany,

[3] **ARTTIC,** Germany

Keywords

Search and Rescue, First Responders, Crisis Management, Emergency Response, USAR, Flash Flood, Wildfire

Extended Abstract

SYNERGISE (SYNERGISE Website, 2024) is an EU-funded research initiative designed to enhance the effectiveness and safety of first responder operations by leveraging cutting-edge technologies. As emergencies and disasters become increasingly complex, SYNERGISE addresses the need for advanced response strategies through the development of integrated robotic solutions and intelligent decision-support systems. These technologies aim to transform the way emergency situations are managed, providing first responders with enhanced capabilities to operate more efficiently in dynamic, high-risk environments.

At the core of SYNERGISE is the creation of the Novel Integrated Toolkit for Collaborative Response and Enhanced Situational Awareness (NIT-CRES), a comprehensive suite of tools and services that empowers response teams by improving situational awareness, communication, and resource management. NIT-CRES enables first responders to perform autonomous and collaborative indoor and outdoor exploration of incident sites, monitor responders' positions and vital signs, assess environmental hazards, and maintain a shared operational picture among various agencies and teams.

Key objectives of the SYNERGISE project include:

1. Developing robotic platforms to support search and rescue, reconnaissance, and hazardous material handling.
2. Designing intelligent decision-support systems that analyse real-time data to provide actionable insights for first responders.
3. Enhancing coordination and communication among response teams through advanced information-sharing technologies.
4. Conducting comprehensive testing and validation of the developed solutions in real-world scenarios to ensure their reliability.

The NIT-CRES toolkit is designed with inclusivity, privacy, security, and ethical considerations, ensuring it adheres to legal and operational standards. It will be tested and validated through a structured programme of collaborative lab tests, field exercises, and technical workshops, enabling search and rescue personnel, fire brigades, emergency medical teams, police, and civil protection agencies to enhance their collaborative response capabilities for managing complex incidents.

Acknowledgements

The project is jointly funded from the European Union's Horizon Europe research and innovation programme; State Secretariat for Education, Research, and Innovation from Switzerland; R2 Network from the United States; the Japan Science and Technology Agency; the Korea Ministry of Science and ICT, and the Korea Electronics and Telecommunications Research Institute. The project started on 1st September 2023 will and run until 28th February 2027.

References

1. (2024, October). Retrieved from SYNERGISE Website: https://www.synergise-project.eu/

TeamUP:

A unified approach to CBRN-E crisis management: TeamUP's role in enhancing first responder capabilities and advancing response technologies

Katerina Valouma, Lazaros Karagiannidis, Eleftherios Ouzounoglou, Thanasis Douklias, George Vosinakis, Angelos Amditis[1], Spyros Kintzios[2], TeamUP Consortium[3]

[1] Institute of Communication and Computer Systems,

[2] Centre for Research and Technology Hellas,

[3] https://cordis.europa.eu/project/id/101121167

Keywords

CBRN-E, Response, Preparedness, Crisis management, First Responders

Extended Abstract

In response to the growing global threat of incidents involving Chemical, Biological, Radiological, Nuclear, and Explosive (CBRN-E) hazards, countries worldwide are investing in strengthening their response capabilities. This need is particularly pressing in Europe, where first responders (FRs) often lack the specialized training and equipment necessary to manage such complex hazards effectively. These limitations hinder their ability to provide timely assistance to victims, conduct proper triage, and implement adequate decontamination procedures. Furthermore, existing resources are constrained, and training is often siloed within individual organizations, leading to a lack of proven procedures, insufficient multidisciplinary collaboration, and minimal knowledge-sharing across agencies. To address these challenges, TeamUP was conceived with the goal of developing a comprehensive framework that enhances the operational capacity of both expert and non-expert first responders in dealing with CBRN-E incidents.

The methodology of TeamUP is grounded in the creation of a unified framework that integrates detailed analyses of current standard operating procedures (SOPs) in CBRN-E preparedness and response. This is coupled with a gap analysis and an assessment of the capabilities of both expert responders and those not traditionally trained to operate in CBRN-E conditions. By merging these findings with the development of innovative technologies, TeamUP seeks to significantly strengthen CBRN-E response capacity and foster cross-sectoral collaboration. The framework defined by TeamUP serves as the foundation for all project activities, guiding the development and evaluation of new technologies aimed at improving CBRN-E incident management.

Implementation of this framework has already begun, starting with a thorough review of modus operandi, existing SOPs, lessons learned from past CBRN-E incidents, and an analysis of the state-of-the-art technologies related to CBRN-E response. As part of this initial phase, two Tabletop eXercises (TTXs) have been conducted to assess existing SOPs and response plans. The first TTX concentrated on decontamination procedures following a CBRN-E event, with special attention given to vulnerable populations. The second simulated a chemical explosion in a

collapsed building, focusing on search and rescue operations, detection, identification, and monitoring (DIM) of hazardous substances, resource management, and communication

between different first responder teams (including fire departments, medical personnel, police, civil protection units, and forensics experts). Each TTX was followed by Small-Scale eXercises (SSXs) that demonstrated field procedures for handling CBRN-E incidents in real-world scenarios.

These early steps are essential for initiating the co-creation process, which emphasizes collaboration among all consortium members in the co-design, co-development, and co-evaluation of innovative solutions. The project has set two main objectives for this process: (1) improving the performance of existing technologies (e.g., increasing detection accuracy) and (2) evaluating how these technologies enhance the capabilities of first responders, particularly those without specialized CBRN-E expertise.

TeamUP is dedicated to developing, integrating, testing, and validating cutting-edge technologies (Figure 1) designed to address the complex challenges posed by CBRN-E incidents in a holistic manner. Key innovations include portable, user-friendly DIM solutions for chemical, biological, radiological, and explosive threats; support systems for search and rescue operations that monitor first responders' health (e.g., wearables and breath analysis); task coordination tools (Worksite Operations App); and advanced digitized triage systems (Digital Tag, mobile applications, and augmented reality services). Additionally, the project is developing a Fast Deployable Mass Decontamination system and smart decontamination monitoring solutions.

Data collected in the field will be processed and analyzed using expert reasoning systems to provide continuous, real-time updates and recommendations for operational guidelines. This is especially vital for ensuring the safety and effectiveness of non-expert responders. A fully integrated and enhanced Incident Management System will further support the coordination of collaborative responses during CBRN-E events. The project will also leverage digital training tools, such as the Digital Scenario Builder, which simulates end-to-end CBRN-E scenarios and incorporates virtual reality (VR) training for first responders.

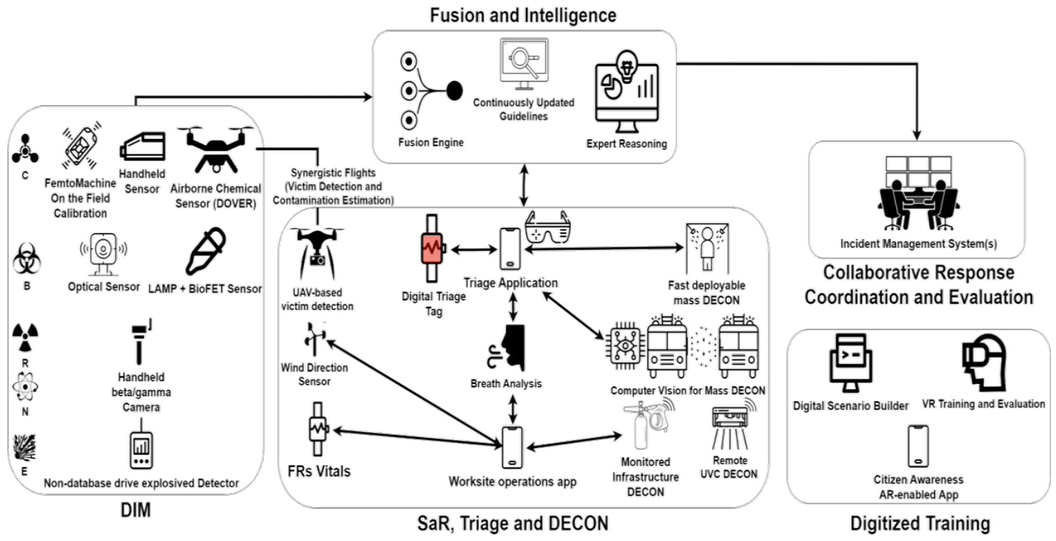


Figure 1: TeamUP high-level architecture

Acknowledgements

This project has received funding from the European Union's Horizon Europe (HORIZON) research and innovation programme under Grant Agreement No. 101121167, project TeamUP. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TREEADS:

TREEADS Project: A Holistic Fire Management Ecosystem for Prevention, Detection and Restoration of Environmental Disasters

Katerina Margariti[1], Maria Zotou[1], Dimitris Kyriazanos[2]

[1] **ACCELIGENCE LTD,** Cyprus,

[2] **NCSR "Demokritos"**

Keywords

Wildfire Management, Wildfire Prevention, Resilience, Innovation

Extended Abstract

The TREEADS project, funded under the Horizon 2020 framework, offers a comprehensive, innovative approach to wildfire management. It integrates advanced technologies such as Artificial Intelligence (AI), Internet of Things (IoT), Unmanned Aerial Vehicles (UAVs), and data analytics to address all phases of wildfire management - prevention, detection, response, and restoration.

A key advancement of the project is its integration of diverse data sources, combining cyber data with information gathered from heterogeneous sensors in the physical environment. This multi-source data fusion enables early detection and timely risk assessment, allowing for preventive measures or mitigation strategies to reduce the catastrophic effects of wildfires. Socio-geographical and socio-economic factors are also included in the risk analysis, providing a more accurate evaluation of fire risks by accounting for both environmental conditions and human factors.

Automation streamlines many steps of firefighting operations, minimizing fire impacts on the environment and human lives. The system is highly interoperable and scalable, utilizing open APIs and standardized data formats to ensure seamless integration of technologies across diverse regions. TREEADS employs a four-layered monitoring approach using multiple UAVs and satellite data to deliver comprehensive forest coverage and real-time insights.

The project also adopts a multi-stakeholder approach, incorporating expert knowledge from forest economics, social-ecological systems, policy, and existing EU initiatives (Arsava et al., 2024).

This collaborative framework ensures TREEADS innovations align with broader European efforts in wildfire management. New technological advancements introduced include fire-resistant materials, innovative insurance models, health monitoring systems, augmented reality (AR) tools for first responders, and UAV-based drone seeding technologies supported by satellite data.

The project's user-friendly interface, available on both desktop and mobile platforms, provides real-time updates on fire conditions and computational analysis results. This ensures that decision-makers and responders have access to the most current information during critical situations (Zapounidis et al., 2024).

TREEADS has already achieved significant milestones, including the development of over 26 innovative technologies. These include real-time AI-based fire risk prediction tools, operational UAV systems for fire detection, and advanced decision support and communication systems for emergency response. AR and VR tools for firefighter training have been validated through several pilot demonstrations.

Currently, eight large-scale pilot sites across seven European countries-Austria, Norway, Spain, Italy, Romania, Greece, and Germany—as well as Taiwan, are validating TREEADS solutions in diverse climatic, geographic, and socio-economic contexts. The pilots focus on forest management, critical infrastructure protection, and biodiversity restoration, ensuring TREEADS solutions are adaptable and scalable for various global environments.

Looking forward, TREEADS will continue refining its technologies and expanding its pilot activities. Future work will enhance data fusion for more accurate fire behavior predictions, further integrate social media and crowd-sourced data to improve situational awareness, and advance restoration efforts using eco-friendly materials and methods. Additionally, TREEADS will expand training and dissemination efforts to foster cross-border collaboration and engage local communities, ensuring widespread adoption of its innovative wildfire management solutions.

By delivering actionable solutions to wildfire risks, improving emergency response efficiency, and promoting sustainable restoration practices, TREEADS is creating a scalable, resilient model for wildfire management in Europe and beyond. The project's outcomes will protect human lives, ecosystems, and critical infrastructure,

Figure 1: TREEADS four layered appraoch

significantly contributing to efforts against climate change-induced disasters.

Acknowledgements

TREEADS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101036926. Content reflects only the authors' view and the Agency/ European Commission is not responsible for any use that may be made of the information it contains.

References

1. Arsava, K. S., Mikalsen, R. F., Fjærestad, J. S., Ulvang, A-I, Li, T., Velanas, P. Margariti, K., Soldatos J., Pascale, C. (2024). TREEADS – Holistic Fire Management Ecosystem for Prevention, Detection, and Restoration of Environmental Disasters, 14th International Symposium on Fire Safety Science IAFSS2023
2. Zapounidis, K., Koidis, C., Sakkos, N., Marinoudi, V., Aidonis, D., & Achillas, C. TREEADS Project: A Holistic Fire Management Ecosystem for Prevention, Detection and Restoration of Environmental Disasters.

03. Effective Management of EU External Borders

BAG-INTEL:

An intelligent system for improved efficiency and effectiveness of the customs control of passenger baggage from international flight arrivals.

BAG-INTEL's Secure-by-Design, Hierarchical-Multi-Cloud, IoT-Edge-Cloud Architecture

Panayiotis A. Michael, Panayiotis D. Tsanakas

National Technical University of Athens, Greece

Keywords

Secure-by-Design Architecture, Hierarchical-Multi-Cloud, IoT-Edge-Cloud Continuum, Defense-in-Depth Architecture

Extended Abstract

The goal of the BAG-INTEL system is to increase the effectiveness and efficiency of customs controls of incoming baggage at international airports without the need of involving extra human resources. By providing robust AI-based information utilization and decision support tools, BAG-INTEL will support the stakeholders of the project (primarily Customs, Police, and Airport Operators) in the detection of baggage containing contraband in a rapid and effective manner. As a result, more contraband will be detected and the cases of unnecessary manual inspections not leading to finding contraband will decrease.

To achieve the above, a Secure-by-Design architecture is being designed by the BAG-INTEL project partners. As a principle, Secure-by-Design introduces security measures early in the lifecycle of the system. The aim is to operate natively with the existing airport infrastructure without requiring additional compensating countermeasures.

The vision of a Multi-Cloud Continuum, integrating airport operations and airport located IoT with governmental clouds and the Common European Data Spaces Cloud, somehow contradicts the best practices followed toward achieving highest security levels: On the one hand, the Cloud-Edge-IoT Continuum offer the benefits of elasticity, high-availability, resilience, and scalability while enabling technical and business convergence; On the other hand, security standards for Information Security Management Systems mandate segregation and development of zones and conduits.

Towards removing this contradiction, our Hierarchical model of the Multi-Cloud, IoT-Edge-Cloud Architecture -- through its hierarchy of clouds, achieves to define a Cloud-Edge-IoT Continuum where security zones are defined. The native layering approach of Hierarchical, Multi-Cloud,

IoT-Edge-Cloud Architecture allows to propose Defense-in-Depth architectural designs, providing multiple security protections in a layered manner, delaying or preventing an attack to the system. Through its optimized-for-security designs, our Secure-by-Design architecture reduces the attack surface, minimizing the interfaces of the system which can be accessed and exposed.

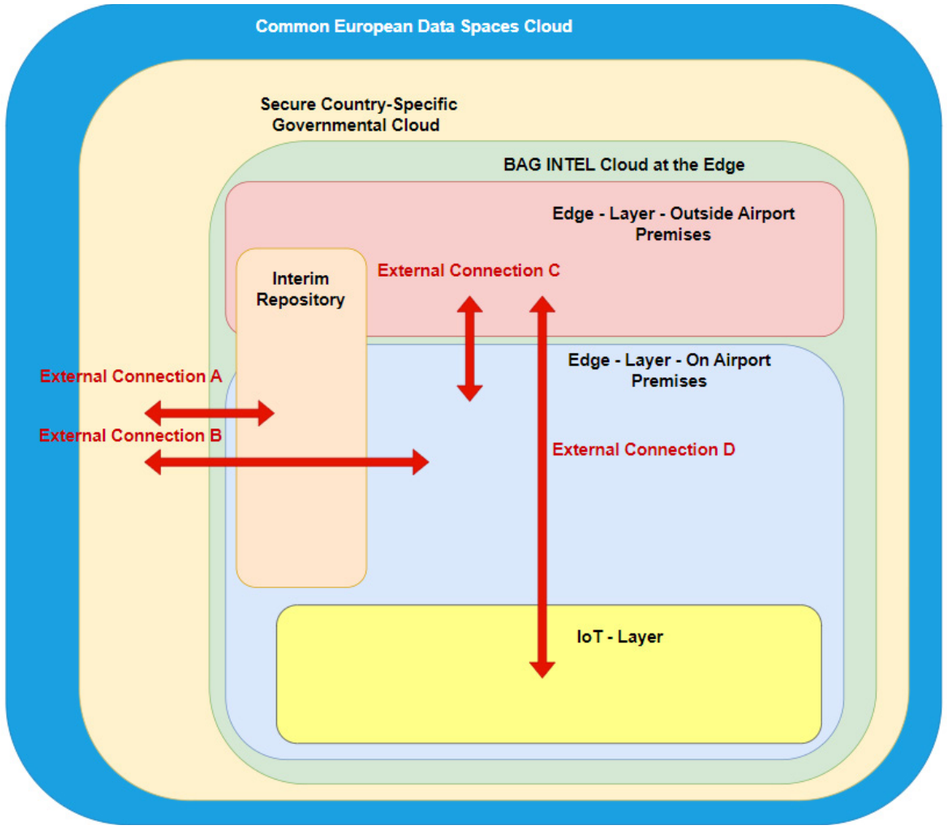


Figure 1: The Secure-by-Design, Hierarchical-Multi-Cloud, IoT-Edge-Cloud Architecture of BAG-INTEL

BAG-INTEL:

An intelligent system for improved efficiency and effectiveness of the customs control of passenger baggage from international flight arrivals.

Legal, Privacy, and Ethical Challenges Addressed by BAG-INTEL

Sotirios Michagiannis

DBC diadikasia, Greece

Keywords

Privacy, Ethics, Personal Data, Video Surveillance

Extended Abstract

In this presentation, the presenters will refer to the legal, privacy, and ethical challenges that the BAG-INTEL project faces due to its nature, the project-related activities, and the framework to be developed. They will also point out the mitigation measures implemented to avoid any potential legal or ethical issues, alongside the actions taken to anticipate them.

The factors identified that may raise issues in terms of privacy and ethics are mostly the human participation, the processing of personal data, especially the video surveillance, the selection of the datasets to be utilized for the purposes of development and evaluation of the BAG-INTEL framework, and the use of the AI technology. The measures identified as appropriate to anticipate such issues are the preparation of consent forms according to the General Data Protection Regulation's provisions and the relevant ethical considerations, following the ethics and privacy protocol as part of the project's data management plan, where specific guidelines are outlined, the adherence to a guide based on the AI Act (Regulation EU 2024/168) and the relevant ALTAI requirements, along with additional monitoring actions, in accordance with the project grant agreement.

CONNECTOR:

CustOms exteNded iNteroperablE Common informaTiOn shaRing environment - CONNECTOR

Souzanna Sofou[1], Antonis Kostaridis[1], Dimitris Diagourtas[1], Marios Moutzouris[1], Spyros Antonopoulos[1], Kiriakos Alevizos[1], Michael Doherty[2]

[1] **SATWAYS Ltd,** Greece

[2] **MD CUSTOMS AND BORDER SECURITY SERVICES LIMITED,** Ireland

Keywords

CISE, e-CISE, EIBM, Customs

Extended Abstract

CONNECTOR's vision is to contribute to the European Integrated Border Management (EIBM) and to the EU Customs Action Plan by i) addressing the need of close cooperation between Customs, Border and Coast Guard Authorities, and ii) by further involving Customs to the Common Information Sharing Environment (CISE) network [1,2] and the Enhanced Common Information Sharing Environment (e-CISE) [3], via the development of the Customs Extended Common Information Sharing Environment (CE-CISE). The CE-CISE Data Model will be based upon the e-CISE Data Model, which extended CISE towards Land Surveillance Operations, introducing Customs domain vocabulary and EIBM common operations like Border Checks & Controlled Deliveries CE-CISE will also take into consideration EUCDM & WCO Customs Data Models.

In addition, CONNECTOR aims to develop, for the first time, an integrated, common and shared risk assessment approach for all IBM Authorities, considering the pan-EU common risk indicators per end user group (Customs, Border and Coast Guards Authorities including FRONTEX). This will serve to secure external EU borders, protect EU citizens from cross-border crime and/or secure the seamless flow of travelers, as recommended in the multiannual strategic policy document.

The CONNECTOR system will be developed in an interoperable technical environment, ensuring close and practical cooperation, as well as information exchange at all levels. The design and development of the CONNECTOR system is based on the analysis of current policy initiatives in EU level (directives, policy and staff documents, guidelines etc.) along with needs, gaps and future views of the end-user groups, going beyond previous EU Horizon initiatives (ANDROMEDA, MARISA, EFFECTOR, etc.), and complying with the EU Societal, Ethical and Legal (SoEL) requirements and regulations.

The CONNECTOR system will be available via an Integration Platform which will integrate the CONNECTOR service and simulate/emulate the legacy C2s of Customs, Border and Coast Guard Authorities, by utilizing the ENGAGE C3i software, offered by Satways Ltd, distributed in Customs, Border and Coast Guard editions. The CONNECTOR system will be validated in a real operational environment, based on well-defined National, Cross border and Transnational use cases jointly defined by Customs, Border and Coast Guards authorities, during three extensive trials (Demonstration and Testing) using a standardised methodology.

This work will also discuss the nature of contribution of the CONNECTOR project to

current policies, including the European Integrated Border Management (EIBM), the European Border and Coast Guard (EBCG) Regulation, European Maritime Security Strategy (EUMSS) and the European Customs Action Plan.

Acknowledgements

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement Number 101121271. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the European Research Executive Agency (REA) can be held responsible for them.

References

1. European Maritime Safety Agency, Directorate-General Joint Research Center (DG JRC) CISE Data Model Documentation (2017), CISE Core Vocabulary Specification (europa.eu), https://emsa.europa.eu/cise-documentation/cise-data- model-1.5.3/
2. ETSI Industry Specification Group (2024) Common information sharing environment service & Data Model (CDM); Data Model; Release 2, https://www.etsi.org/deliver/etsi_gs/CDM/001_099/005/02.01.01_60/gs_CDM005v020101p.pdf
3. ANDROMEDA Horizon 2020 project (Grant Agreement number:833881), Deliverable D3.1 e-CISE Data Model description (2020), https://www.andromeda-project.eu/downloads/deliverables/D3.1.pdf

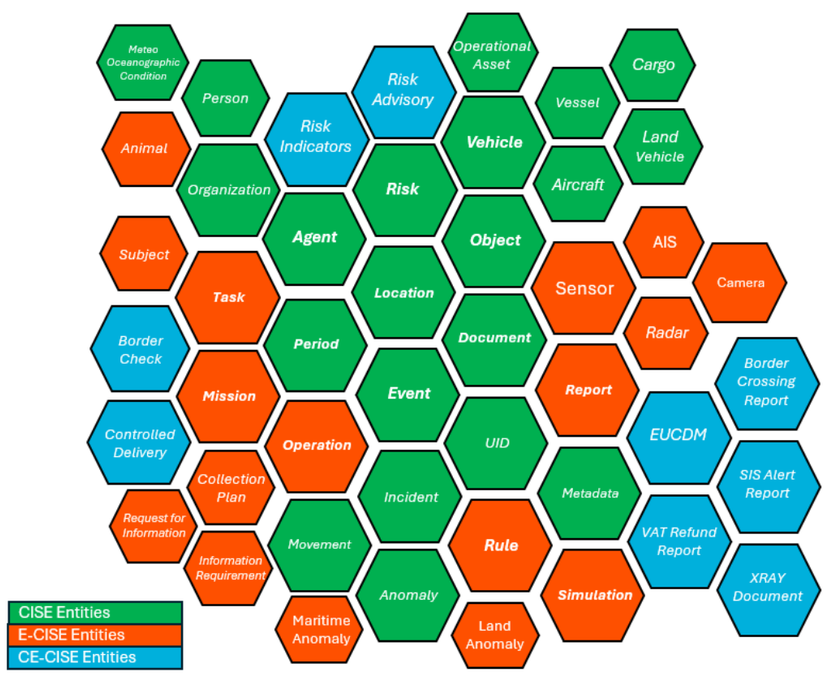


Figure 1: Data Model Evolution from CISE [1], to e-CISE [3] and CE-CISE.

EURMARS:

Leveraging Context-Aware Microtasks and Feedback Loops to Improve Decision Support in Border Management Operational Procedures

Christos Didachos[1], Georgios Mourkousis[1], Matthaios Protonotarios[1]

[1] **Hardware and Software Engineering Ltd,** Greece

Keywords

Border Surveillance, Natural Language Processing (NLP), Decision Support Systems, Semantic Similarity, Sentiment Analysis

Extended Abstract

In the modern era, information technology utilisation has gained significance if not 'is being used' in the profound socio-political sphere in Europe particularly, stability and security of the European continent and peace in the region with regards to internal and external threats. When it comes to the European security environment, there are many concerns such as illegal crossings, human and drug trafficking and more illegal activities that require greater attention on the borders of the EU. Leveraging these new tools, officers are able to simultaneously oversee and implement border control, threat assessment, and threat management most effectively1 (Huxtable, 2021). In this way these systems do not only improve situational awareness but also support situation management through data originating from various sources to enable improved border security management.

To enhance the efficiency of operations, as well as their capability to mitigate risks, these systems must be complemented with closer cooperation among national, regional and EU-level authorities. In this regard, projects like EURMARS2 (Kriechbaum-Zabini, 2023) aim to create better cooperation between different authorities at the European Union borders. This initiative introduces new design features for global borders that can improve security by enhancing monitoring and surveillance. EURMARS uses comprehensive information acquisition systems including high altitude platforms, satellites, unmanned vehicles and ground sensor networks in which every platform contributes for a holistic multi-sensored usage. The integration of advanced Command and Control (C2) systems, as demonstrated in platforms like CAMELOT3 (Pérez et al., 2021), highlights the importance of interoperability between multiple domains and assets, ensuring that unmanned systems and other resources can be effectively coordinated for enhanced situational awareness and mission success.

A key technological advancement in projects integrating decision support functionality, like EURMARS, is the integration of Natural Language Processing (NLP), which plays a critical role in decision-making processes. NLP plays a crucial role in suggestion systems by interpreting unstructured text data, such as user reviews, product descriptions, and real-time communication, which enhances decision-making processes even in critical areas like border security4 (Shalom et al., 2021). These systems are also able to understand human language, whether it is in reports, memoranda, commands or conversations and extract meaning from them. In addition, this functionality can

enable decision support systems to assess user participation such as whether input given is positive, negative or neutral which increases speed or accuracy of operational procedure. A key objective in enhancing the security of border management systems is to improve their recommendation capabilities. By efficiently analyzing past strategies and adjusting to changes in the operational environment, these systems can provide more accurate and timely suggestions.

The EURMARS Decision Support System (DSS) is developed to assist in handling threats and improving decision-making capabilities. The DSS receives messages of potential security threats through a risk assessment process. If a potential threat is detected and visualized on the C2 platform, then the DSS provides support to the user not only by offering Common Operational Procedures (COPs) specific to each threat type but also by helping users navigate the appropriate response strategies. These procedures are further broken down into context-aware microtasks, guiding users step-by-step through the threat management process.

The DSS is equipped with a learning mechanism that evolves based on user feedback and actions taken during and after events. For instance, after resolving a threat, the officer can review the entire course of actions and the DSS's recommendations. This offers the officer the capability to refine responses, suggest new or updated microtasks, and further enhance future threat resolution processes. Importantly, while the system suggests microtasks related to COPs, it does not alter the COPs themselves but offers additional details and improvements to support user actions.

Additionally, the DSS provides a feedback system where users can vote on the effectiveness of the system's suggestions. During the threat-handling process, the user can provide fast feedback (e.g., with a simple "positive" or "negative" vote), while more detailed feedback after the event carries additional weight. This makes the DSS capable of understanding the most effective combinations of microtasks. More so, there is also the element of Natural Language Processing (NLP), which collects and compares feedback and sorts similar activities to further improve the system's recommendations. All this results in a recommendation system that helps rather than replaces the people who use it, making sure that the most optimal assistance for the subsequent actions is always at hand.

The below flow Diagram, represents the structure of the DSS system.

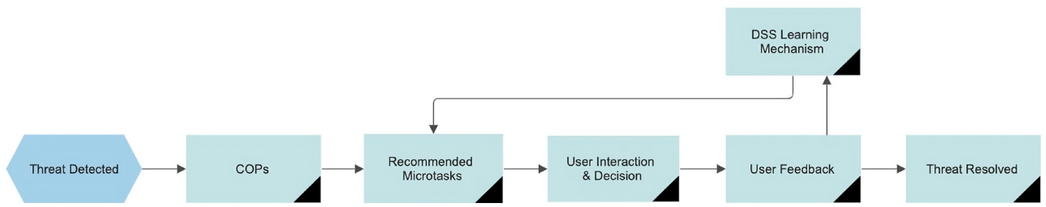


Figure 1

Acknowledgements

EURMARS project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073985, EC HORIZON

References

1. Huxtable, L. (2021). Artificial Intelligence -based capabilities for the European Border and Coast Guard.
2. Kriechbaum-Zabini, A. (2023). EURMARS An advanced surveillance platform to improve the EURopean Multi Authority BordeR Security efficiency and cooperation. In RISE SD 2023: Security and Defense 2023 (pp. 185-186).
3. Pérez, F. J., García, A., Garrido, V. J., Esteve, M., & Zambrano, M. (2021). C2 Advanced Multi-domain Environment and Live Observation Technologies: CAMELOT Project. International Journal of Computers Communications & Control, 16(6).
4. Shalom, O. S., Roitman, H., & Kouki, P. (2021). Natural language processing for recommender systems. In Recommender Systems Handbook (pp. 447-483). New York, NY: Springer US.

ODYSSEUS:

Unobtrusive Technologies for Secure and Seamless Border Crossing for Travel Facilitation

Monica Florea[1]

[1] **Software Imagination and Vision SRL,** Romania

Keywords

Seamless Border Crossing, Land and Water Borders, Behavioural Authentication, Unobtrusive Vehicle Scanners, Drones

Extended Abstract

ODYSSEUS - Unobtrusive Technologies for Secure and Seamless Border Crossing for Travel Facilitation is an innovative EU project, funded under the call HORIZON-CL3-2021-BM-01-03, with the major objective of improving both the border checks for travel facilitation across external borders and the experiences for the passengers and border authorities' staff through the implementation of smart digital solutions.

The project, coordinated by Software Imagination & Vision SRL Romania, and involving fourteen EU and non-EU partners from twelve countries, aims to achieve the following objectives:

- **DESIGN and DEVELOP** a unifying platform that enables seamless, fully non-stop border crossing in a highly secure manner, assisting LEAs with automated, reliable and accurate border checks
- **ADVANCE** the identification and control capabilities of Border Authorities through robust and reliable identity verification mechanisms introducing an EU mobile (virtual) passport protected by continuous behavioural authentication
- **IMPROVE** the border control checks without stopping cargos and vehicles through safe, unobtrusive and portable screening based on X-Ray backscatter technology, UAV-assisted image processing and AI based data analytics
- **VALIDATE** the effectiveness of the proposed ODYSSEUS platform through its demonstration in real-life environments in two diverse landscapes and various operational environments (inside a train, on the road, onboard a ship in a port area)
- **SPEED UP** the rapid uptake by relevant security stakeholders of the ODYSSEUS innovations through wide communication, scientific dissemination and targeted commercial exploitation activities coupled with contributions to relevant standardisation bodies.

The solution offered by ODYSSEUS project for the border authorities and for citizens blends multiple devices and technologies:

- Traveller enrolment:
  1. Creation of Digital and Virtual Passport- Mobile Wallet App
  2. AI-powered Continuous Behavioural Authentication
- Vehicles screening:
  1. Non-Obtrusive and Safe X-Ray Technologies for Vehicle Scanning
  2. UAV-Assisted Vehicle Scanning based on Thermal and High-Resolution Cameras
- Border Crossing:
  1. Seamless Biometric Identity Solutions in Border Crossing Scenarios
  2. Faceless GDPR Compliant Travellers Counting
- Informed decision making:
  1. Multi-Modal Fusion and Decision Support System equipped with XAI

These technologies are integrated within the ODYSSEUS platform visualization features, that delivers insightful reports and analytics based on the functionality of the components defined in the project.

The ODYSSEUS platform will be demonstrated and evaluated through three real-world scenarios: pilot at land, pilot at water and pilot at train, and the benefits of the project will thus be exploited in both land and water environments. The Customs and Border Protection and European citizens travelling abroad are the ODYSSEUS project's primary end users.

Combined with secure, discreet X-ray inspection and UAV-assisted thermal scanning of the vehicle, the solution in the **'Pilot at the Land Border'** use case is that the vehicles can cross borders non-stop while undergoing rigorous checking. Passengers will need to access their Mobile Passport and actively complete the identity verification process while the ODYSSEUS platform is notified which individual is about to cross the border. UAVs fly over vehicles on board and those approaching border controls points to identify potentially unregistered travellers. In addition, vehicles entering and leaving the borders are inspected using X-ray scanning to detect possible illegal/illegal goods and substances.

Through ODYSSEUS, passengers receive seamless identity verification, enabling non-stop port entry and exit, and border authorities discreetly inspect vehicles and cargo in **'Pilot at the Water Border'** use case. Mobile Passport allows passengers to enter/exit ports/boats without stopping and can automatically present all relevant documents such as vaccination certificates and visa documents to border authorities. Behavioural Authentication technology works with Digital Travel credentials.

Also, in the final use case, **'Pilot at the Train'** ODYSSEUS will deploy new identity verification technology to enable EU travellers to seamlessly cross checkpoints non-stop.

04. Resilient Critical Infrastructures and Smart Cities

ATLANTIS:

AI at the service of EU CI protection: The ATLANTIS approach

Nikos Konstantinou[1], Theodoros Semertzidis[1], Jolanda Modic[2], Georgia Dede[3], Gianfranco Caputo[4], Cristian Raul Vintila[5], Artemis Voulkidis[6], Gabriele Giunta[7]

[1] **Centre for Research and Technology Hellas,** Greece

[2] **Institute for Corporate Security Studies,** Slovenia

[3] **Netcompany Intrasoft S.A.,** Luxembourg

[4] **LINKS Foundation,** Italy

[5] **SIEMENS,** Romania

[6] **Synelixis Solutions, S.A,** Greece

[7] **Engineering Ingegneria Informatica S.p.A.,** Italy

Keywords

Resilience, Cyber-Physical Systems, Systemic Risks, Risk Management, Situational Awareness, Explainable AI, Critical Infrastructures

Extended Abstract

The ATLANTIS project is a collaborative initiative involving 39 European partners aimed at enhancing the resilience and security of Critical Infrastructures in Europe (ECIs) against both natural hazards and cyber-physical-human threats. By focusing on improving situational awareness, developing adaptable security measures, and fostering cooperation among stakeholders, ATLANTIS seeks to create a robust framework for managing systemic risks.

ATLANTIS starts by modelling interdependencies among ECIs to enhance their resilience and security at local, regional and pan-European level. Understanding and acknowledging these connections is crucial for anticipating cascading effects, where disruptions in one system can trigger widespread impacts across others. Different types of dependencies, including physical and cyber, are mapped, and magnitude modelling is applied to assess the overall impact of potential failures. Practical examples illustrate how disruptions can propagate, highlighting the urgency for adopting effective risk management toolchains to ensure preparedness and continuity in critical infrastructure operations.

Following the modelling phase, ATLANTIS focuses on different aspects of systemic security management, defining multiple components, each one contributing to the overall risk management process proposed by the project

The Awareness and Comprehension Framework (ACF) and the Cyber-Physical-Human Enriched Decision Support System (DSS) are designed to bolster the resilience and security of ECIs. The ACF employs advanced computational methods to assess threats and enable proactive risk management by analysing diverse data sources, one of such methods and tools being the Situational Awareness Framework for Enhancing CI Resilience (SAFER). It analyses CIs' interdependencies, identifies systemic threats, facilitates information sharing, and suggests preventive actions. The DSS builds upon this situational awareness, offering real-time threat assessments, incident tracking, and risk mitigation suggestions. For example, a practical scenario involving cross-border rail transport of hazardous goods between Italy and Slovenia demonstrates the system's ability to manage incidents such as freight disappearance, environmental threats, public order disturbances, and cyber-attacks, featuring real-time threat detection and resolution.

To further enhance resilience at a systemic level, ATLANTIS has developed a Risk Reduction and Incident Mitigation (RRIM) framework. This tool addresses major natural hazards and complex attacks that could disrupt critical infrastructure operations. The RRIM framework incorporates advanced machine learning algorithms to assess crisis data trends, generating recommendations based on a continuously updated knowledge base. By utilizing real-time data streams, the system provides incident classifiers, producers, and recommendation engines that interact to predict and respond to cyber-physical threats. A user-friendly interface allows for seamless interaction, enabling updates to the knowledge base and offering explainable, data-driven recommendations to minimize risks in critical infrastructure operations.

The ATLANTIS project also addresses vulnerabilities in Global Navigation Satellite Systems (GNSS), which are widely used for positioning and time synchronization in critical infrastructures. It focuses on enhancing resilience against GNSS threats, including jamming, spoofing, and meaconing, which can disrupt services in sectors such as aviation, telecommunications, and finance. By employing modern AI-based detection techniques, ATLANTIS analyses the GNSS power spectrum through time-frequency representations to detect and classify interference [1]. Using convolutional neural networks (CNNs), the system can recognize various jamming types from spectrogram images. Furthermore, ATLANTIS explores the potential of 5G as a backup solution for GNSS, ensuring continuous Position, Navigation, and Timing (PNT) services. Use cases such as positioning in tunnels and time synchronization for financial hubs demonstrate the project's practical applications in maintaining critical infrastructure resilience.

Additionally, the Explainable AI (XAI) tools developed within the project aim to enhance transparency and trust in AI systems used for Critical Infrastructure Protection. These tools provide clear, human-readable explanations of AI decisions, facilitating better collaboration between AI systems and infrastructure operators. The XAI methods employed in ATLANTIS help anticipate emerging risks and improve user acceptance of AI-driven decisions. Techniques such as SHAP [2] and Grad-CAM [3] are utilised to interpret model decisions, striking a balance between theoretical grounding and heuristic approaches. Key challenges include ensuring explainability without compromising security or privacy, as exposing AI decision processes can lead to confidentiality risks. Ultimately, results are aggregated into a dashboard, providing critical infrastructure operators with a clear view of AI-driven insights for informed decision-making, thereby fostering better coordination between cyber and physical infrastructure systems.

Finally, the ATLANTIS project integrates DevSecOps practices to ensure resilience in the deployment of its frameworks, emphasizing the seamless incorporation of security throughout the software development lifecycle. By utilizing technologies such as Kubernetes for container orchestration and GitLab CI/CD for automation, the project ensures continuous integration, delivery, and deployment. The incorporation of static (SAST) and dynamic (DAST) application

security testing tools enhances the security posture by detecting vulnerabilities early in the development process [4]. These practices enable automated, scalable, and secure deployments, fostering collaboration and reducing operational risks while maintaining service resilience.

In conclusion, ATLANTIS emphasizes data-driven approaches and collaboration among stakeholders to improve security and decision-making in the protection of critical infrastructures.

Acknowledgements

This project has received funding from the European Union's Horizon Europe framework programme under grant agreement No.101073909.

References

1. Elango, A., Ujan, S., & Ruotsalainen, L. (2022). Disruptive GNSS signal detection and classification at different power levels using advanced deep-learning approach. In Proceedings of the ICL-GNSS 2022
2. Lundberg, S., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In Proceedings of the 30st International Conference on Neural Information Processing Systems (NIPS 2017) (pp. 4765–4774).
3. Selvaraju, R. R., Cogswell, M., Das, A., Vedantam, R., Parikh, D., & Batra, D. (2017). Grad-CAM: Visual explanations from deep networks via gradient-based localization. In Proceedings of the IEEE International Conference on Computer Vision (pp. 618–626).
4. Aydos, M., Aldan, Ç., Coşkun, E., & Soydan, A. (2022). Security testing of web applications: A systematic mapping of the literature. Journal of King Saud University - Computer and Information Sciences, 34(9), 6775–6792.

SUNRISE:

Strategies and Technologies for UNited and Resilient Critical Infrastructures and Vital Services in Pandemic-Stricken Europe

Matjaž Tavčar[1]

[1] **University Medical Centre Ljubljana**, Slovenia

Keywords

Resilience, Critical Infrastructure, Cooperation, Strategy

Extended Abstract

As Europe continues to recover from the COVID-19 pandemic, its citizens and governments are looking ahead to futureproof society's lifeline structures. The EU-funded SUNRISE project aims to ensure greater availability, reliability, and continuity of critical infrastructures in Europe including transport, energy, water, and healthcare.

From October 2022 to September 2025, 41 partner organisations will work together to develop a suite of novel technologies and solutions that will improve the resilience of these critical infrastructures against the impact of pandemics and other major risks. Coordinated by the Spanish arm of global cloud and digital service company, ATOS IT Solutions and Services Iberia SL, the SUNRISE project has been awarded €10m in funding by the EU's Horizon Europe research and innovation programme. The SUNRISE consortium includes 18 public and private CI operators and authorities.

Objectives:

- Facilitate active collaboration among CIs within and across European borders, within and across different sectors, between public and private stakeholders
- Identify pandemic-specific vital services and CIs in Europe, their interactions and dependencies, the risks and cascading effects among them, and effective countermeasures at European level.
- Develop a comprehensive strategy and a set of mature technologies for CI resilience and business continuity in a pandemic, following the Quintuple Helix innovation model.
- Pilot the new strategy and technologies in real-world conditions across Europe.
- Enhance knowledge, awareness, and capacities for unity and resilience in Europe.

New solutions to be developed:

- Facilitate **collaboration, cooperation, and unity** among public and private critical infrastructure (CI) operators and competent authorities across different critical sectors and across entire Europe, discouraging them to work in isolation.
- Understand **interdependencies** between the CIs and the associated **risks and cascading effects** among them, enabling the definition of **effective measures** that are aligned with the needs of societies, economies, and climate, thereby providing for a better **preparedness and resilience** to future health crises.
- **Minimize the exposure of essential workers** with a solution for a risk-based access control to critical facilities.
- Better **forecast and manage rapidly**

changing demands for vital resources (physical, digital, and human).

- Increase **cyber-physical resilience** to ensure a reliable, robust, and continuous operation of digital services.
- **Remotely inspect physical infrastructure** to ensure resilience and continuity of critical services during periods with less available skilled workers while addressing more frequent and more extreme natural disasters.

One of the important features of the project is addressing the **prevention of domino effects among CIs in crisis.**

Cooperation among critical infrastructure entities is crucial for ensuring the resilience and security of essential services such as energy, water, transportation, telecommunications, and healthcare. By working together and sharing information and resources, critical infrastructure entities can effectively identify and address vulnerabilities, threats, and potential disruptions.

One of the goals of the SUNRISE project is providing strategy for collaboration among critical infrastructure sectors and stakeholders that can help in various ways, including:

- **Information Sharing:** Sharing threat intelligence, best practices, and lessons learned among critical infrastructure entities can enhance situational awareness and improve incident response capabilities.
- **Coordination:** Coordinated planning and response efforts can ensure a unified and effective response to incidents that impact multiple sectors or regions.
- **Resilience Planning:** By collaborating on resilience planning and risk management strategies, critical infrastructure entities can better prepare for and mitigate the impact of disruptive events.
- **Cross-Sector Partnerships:** Building partnerships across different critical infrastructure sectors can enable a more holistic approach to security and resilience, considering interdependencies and cascading effects.
- **Training and Exercises:** Conducting joint training exercises and simulations can help improve coordination, communication, and response capabilities among critical infrastructure entities.

Another very important issue we are addressing is **cross-border cooperation.** During crisis it can easily happen that resources within country borders do not suffice and neighbouring facilities will be needed. At present cross-border cooperation is very bureaucratic and takes too much time to organize.

Therefor overall, fostering a culture of cooperation and collaboration among critical infrastructure entities is essential for enhancing overall resilience and security in today's interconnected and complex environment.

With these, SUNRISE significantly, directly, and immediately increases resilience of CIs, improves safety, wellbeing, and trust of citizens, and supports the move towards climate-friendly operations across Europe.

Acknowledgements

I would like to thank authors of webpage sunrise-europe.eu, for the template of presentation of the project and description partly used in this abstract. I would also like to thank Aljoša Pašić, project leader for inviting me to present the project at the conference.

References

1. https://sunrise-europe.eu/about/
2. Tavčar, M. (2024, May 22nd) Preventing Domino Effects in Crisis https://sunrise-europe.eu/2024/05/22/preventing-domino-effect-in-crisis/

TESTUDO:

Autonomous swarm of heterogeneous resources in infrastructure protection via threat prediction and prevention

Stella Parisi[1], Konstantinos Ioannidis[1], Stefanos Vrochidis[1], Ioannis Kompatsiaris[1]

[1] **Centre for Research and Technology Hellas**, 6th km Charilaou-Thermi Rd, P.O. Box 60361, Thermi, GR 57001 Thessaloniki, Greece

Keywords

Critical Infrastructure Protection, Emergency Services, Evaluation of Threats and Vulnerabilities, Robotics, Tele-Robotics & Autonomous Systems, Surveillance of Environment, Autonomous Resource Allocation

Extended Abstract

In recent years, Europe has faced a range of complex challenges, both internally and in its adjacent territories, which have affected the stability, security, and prosperity of local communities [1]. These changes, combined with technological advancements and emerging threats, pose significant risks to Critical Infrastructures (CI). Such structures are vital for the security, economic growth, innovation and well-being of European citizens. Ensuring their reliable, resilient, and autonomous operation is paramount, particularly in light of the European Commission's Security Union Strategy, which emphasizes the importance of safeguarding such systems [2]. However, as CIs become more digitized and interconnected, they are increasingly vulnerable to sophisticated threats, including cyberattacks and physical disruptions [3]. The failure of one CI can cascade through interconnected networks, potentially endangering both the infrastructure and the first responders involved in managing such incidents [4].

To address these challenges, CI operators require innovative solutions that can operate autonomously, adapt to varying operational needs, and support effective decision-making in the face of hazardous events [5]. Despite the availability of mature technologies that assist in CI operations and risk mitigation, there is currently no integrated, holistic solution that leverages heterogeneous autonomous assets for comprehensive CI protection. This gap presents a significant opportunity for technological advancement.

The TESTUDO project is designed to fill this gap by delivering an innovative prototype solution for CI protection that emphasizes autonomy, long-term deployment, and resilience. The project aims to design, implement, validate, and deliver a system capable of meeting diverse operational challenges, utilizing a three-pillar approach:

1. Novel sensing components for enhanced and diverse detection capacities, including the use of dynamic sensors on unmanned assets and fixed sensors in remote and challenging environments.
2. AI-driven knowledge extraction and machine learning (ML) frameworks to enhance decision-making capabilities.
3. Advanced prevention and prediction models to minimize the impact of hazardous events and support recovery efforts.

These technologies will collectively create a robust and flexible CI monitoring and protection system, capable of autonomous operation in complex and unpredictable environments as depicted in Figure 1.

The primary objective of TESTUDO is to deliver a prototype at Technology Readiness Level 7 (TRL-7), which will be capable of autonomously managing CI protection in challenging environments. TESTUDO's two strategic objectives are Autonomy on the Platform (AoP) and Autonomy on the Edge (AoE). AoP will focus on integrating autonomous functionality into a system of heterogeneous assets, such as unmanned vehicles (UxVs) and a network of fixed sensors. This platform targets to enhance preparedness, prevention, and response capabilities by enabling detection, identification, and coordinated response to potential threats. AoE, on the other hand, will deliver AI-based offline cognitive capabilities that can operate in remote areas with limited or no connectivity, ensuring that the system remains functional even in the absence of communication links.

By leveraging state-of-the-art AI technologies, TESTUDO will enable high-level autonomy, reducing the need for human intervention in CI protection operations. The system will also incorporate a variety of advanced sensing and detection technologies, ensuring a robust and reliable monitoring framework capable of identifying threats early and supporting effective prevention and mitigation strategies. Through a combination of real-time decision-making tools, secure communication systems, and AI-powered threat assessment models, TESTUDO will deliver a comprehensive framework for enhanced situation awareness and optimal response to hazardous incidents.

Moreover, each TESTUDO prototype will be tested and validated through in short and long-term deployments in one operational trial and two large-scale and cross-sectorial trials. These trials will demonstrate the system's ability to handle a wide range of threats to CI, such as natural disasters, terrorist attacks, and incidents involving hazardous materials. Each version of the prototype will undergo rigorous testing in both short-term and long-term scenarios to evaluate its ability to protect, prevent, and predict critical events and validate the robustness, flexibility, and resilience of the TESTUDO solution. The trials will provide critical information to CI operators and first responders, ensuring that the system can function autonomously over extended periods and adapt to varying operational conditions.

In conclusion, TESTUDO will demonstrate a highly flexible and modular platform that can be tailored to the specific needs of different CI operators. The ultimate goal is to provide a scalable, autonomous, and resilient solution for the long-term protection of critical infrastructures across Europe.

Acknowledgements

TESTUDO project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121258. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Un-ion or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

1. Felice, F., Baffo, I., & Petrillo, A. (2022). Critical Infrastructures Overview: Past, Present and Future.Sustainability. https://doi.org/10.3390/su14042233.
2. EUR-Lex - 52020DC0605 - EN - EUR-Lex (europa.eu)

3. Aradau, C. (2010). Security That Matters: Critical Infrastructure and Objects of Protection. Security Dialogue, 41, 491 – 514. https://doi.org/10.1177/0967010610382687.

4. Gheorghe, A.V., & Schläpfer, M. (2006). Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures. 2006 IEEE International Conference on Systems, Man and Cybernetics, 1, 580-584.

5. Matthews, G., Reinerman-Jones, L., Barber, D.J., Teo, G., Wohleber, R.W., Lin, J., & Panganiban, A.R. (2016). Resilient autonomous systems: Challenges and solutions. 2016 Resilience Week (RWS), 208-213.

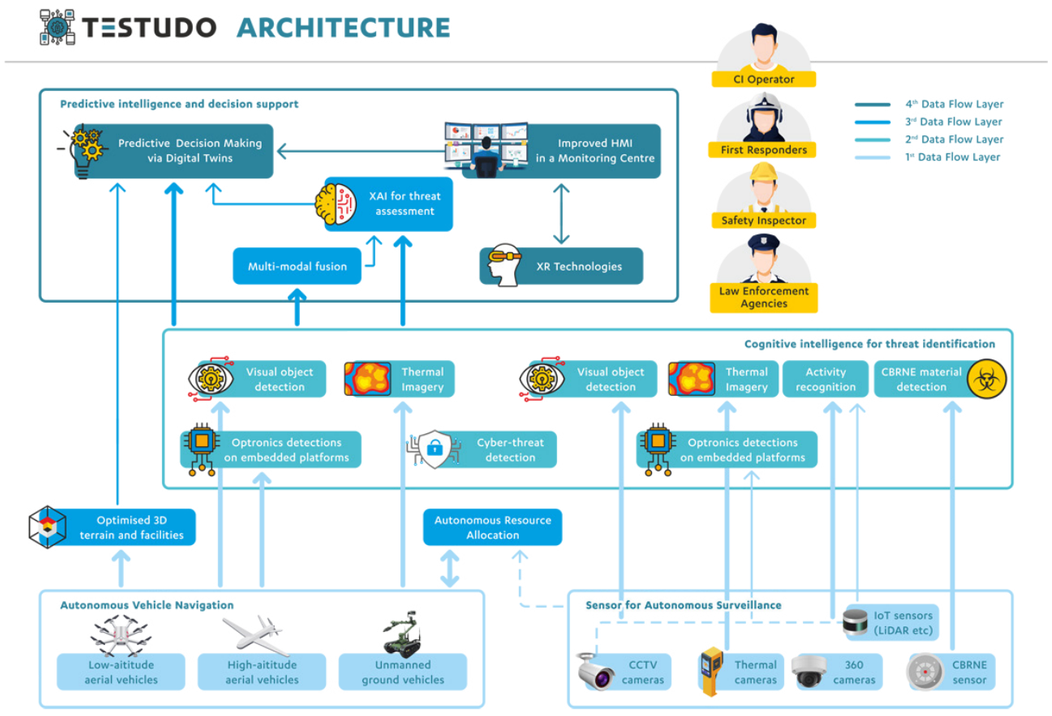


Figure 1: Preliminary, high-level depiction of the TESTUDO architecture.

05. Increased Cybersecurity

ELECTRON:

rEsilient and seLf-healed EleCTRical pOwer Nanogrid

Aikaterini Karampasi[1], Panagiotis Radoglou-Grammatikis[1], Pavlos Bouzinis[2], Thomas Lagkas[3], Panagiotis Sarigiannidis[1]

[1] **Department of Electrical and Computer Engineering,** University of Western Macedonia, Campus ZEP Kozani, 50100, Kozani, Greece,

[2] **MetaMind Innovations,** Kila, 50100 Kozani, Greece,

[3] **Department of Computer Science,** Democritus University of Thrace, Kavala Campus, 65404, Kavala, Greece

Keywords

Cybersecurity, Dynamic Risk Assessment, Energy, Smart Electrical Grid, Self-healing, Software-Defined Networking

Extended Abstract

ELECTRON refers to an integrated platform which is capable of detecting and mitigating potential cyberattacks in a timely manner, combining a set of cybersecurity and energy defensive mechanisms.

As illustrated in Figure 1, the ELECTRON architecture relies on the SDN architectural model (Amin, Reisslein, & Shah, 2018). In particular, the SDN model consists of four main planes, namely (a) Data Plane, (b) Control Plane, (c) Application Plane and (d) Management Plane. The Data Plane refers to EPES entities/devices that are connected to hardware or software SDN switches. It is noteworthy that the EPES devices/entities are not considered as part of the ELECTRON architecture but assets of the use case/pilots that interact with the ELECTRON components. On the other hand, the SDN switches are an essential ingredient of the ELECTRON architecture since many ELECTRON components use the SDN technology. Next, the Control Plane is characterised by the presence of the SDN Controller (SDN-C), which is responsible for managing the network elements of the Data Plane through the southbound Application Programming Interface (API). The Application Plane includes applications that guide and communicate with the SDN-C in order to apply efficient policies with respect to the entities of the data plane. For this purpose, northbound APIs are utilised regarding the communication between the applications and the SDN controller, such as REpresentational State Transfer (REST), which will be adopted in the context of ELECTRON. Finally, the Management Plane is a cross-layer block responsible for the deployment, configuration and management of the various entities/devices and components of the other planes.

Based on the aforementioned remarks, within ELECTRON, the Data Plane will include both hardware and software SDN switches that will interconnect the EPES entities/devices, such as Programmable Logical Controllers (PLCs), Remote Terminal Units (RTUs), smart meters, Phasor Measurement Units (PMUs), etc. with the SDN controller. In the context of ELECTRON, OpenFlow will be used as a southbound protocol, while Aruba hardware SDN switches and Open vSwitch (OVS) will also be used based on the characteristics and the requirements of the ELECTRON use cases/pilots. Next, regarding the Control Plane, multiple SDN-Cs will be deployed and used, thus avoiding a single point of failure, which is a severe security issue for the SDN networks due to potential Denial of Service (DoS) and Distributed DoS (DDoS) attacks. The SDN Controllers will be synchronised and coordinated with each through the Synchronisations and Coordination Service (SCS) of the Management Plane. The Application Plane refers to the ELECTRON core, comprising several cybersecurity and energy protection components that will guarantee the security and resilience of the EPES infrastructure/organisation. In particular, the ELECTRON components are separated into four main logical frameworks: (a) Collaborative Risk and Certification Framework (BORDER), (b) Cybersecurity and Privacy-Preserving Framework (CYPER), (c) Nanogrid-based Prevention and Mitigation Scheme (BRIDGE) and (d) Personnel Training and Certification Environment. Each of the previous frameworks includes multiple functional components that cooperate with each other in order to protect adequately the various cyber-physical risks against the energy sector. In particular, BRIDGE consists of three components related to the collaborative and dynamic risk assessment and cybersecurity certification. Next, CYPER includes eight components pertaining to the intrusion/anomaly detection and correlation. BRIDGE consists of four main components focusing on intrusion/anomaly mitigation, taking full advantage of the SDN technology and electricity-related mitigation actions. Finally, PRINCE focuses on cybersecurity evaluation and certification educational and training activities with respect to the EPES personnel. Management Plane includes services related to the orchestration, deployment, interconnection and security of the ELECTRON components of each previous logical framework. In particular, based on the characteristics, requirements and scenarios of each use case/pilot (Annex B), the appropriate components will be deployed, including the corresponding User Interface (UI) environments (i.e., Dashboards). Moreover, it is worth mentioning that this layer also refers to penetration testing services that will check the security level of the ELECTRON components themselves, utilising both commercial tools and services coming from the ELECTRON partners and opensource technologies such as Nmap, Nikto and OpenVAS.

Finally, it is noteworthy that ELECTRON architecture is characterised by eight functional layers: (a) SDN-Layer, (b) Electrical Layer, (c) Islanding and Restoration Layer, (d) Intelligence Layer, (e) Resilience Layer, (f) Information Layer, (g) Platform Layer and (h) Authority Layer. The functionality behind these layers relies on the components of the logical frameworks (i.e., BORDER, CYPER, BRIDGE and PRINCE) and the SDN solution. In particular, the SDN Layer refers to the presence of the SDN controller managing and controlling the SDN network. The Electrical Layer refers to the EPES entities/devices interconnected with the SDN switches. Next, the Islanding and Restoration Layer denotes the functionality of the BRIDGE components that can form autonomous microgrids/nanogrids and restore the main electrical grid. The Resilience Layer refers to the capabilities of the ELECTRON components to ensure the normal operation of the electrical grid in case of critical cyberattacks. This is achieved, through the dynamic and collaborative risk assessment of BORDER and the mitigation and prevention services of BRIDGE and the SDN-C. The Information and Intelligence Layers refer to the CYPER components that use and handles various kinds of data in order to detect and disseminate timely potential intrusions and anomalies. The Platform Layer implies the capability of the ELECTRON components to be provided and used as Software as a Service (SaaS) model, thus showing the ELECTRON scalability. Finally, the Authority Layer refers to the creation

of a cybersecurity lighthouse based on the certification and standardization mechanisms and guidelines that will be extracted by the outcomes of the project.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021936 (ELECTRON).

References

1. Amin, R., Reisslein, M., & Shah, N. (2018). Hybrid SDN networks: A survey of existing approaches. IEEE Communications Surveys & Tutorials, 20, 3259–3306.
2. Bagyalakshmi, G., Rajkumar, G., Arunkumar, N., Easwaran, M., Narasimhan, K., Elamaran, V., . . . Ramirez-Gonzalez, G. (2018). Network vulnerability analysis on brain signal/image databases using Nmap and Wireshark tools. Ieee Access, 6, 57144–57151.
3. Case, J. D., Fedor, M., Schoffstall, M. L., & Davin, J. (1989). Simple network management protocol (SNMP). Tech. rep.
4. Duffy, J. (2014). Cisco reveals OpenFlow SDN killer; OpFlex protocol for ACI offered to IETF, OpenDaylight. Network World.
5. Karangle, N., Mishra, A. K., & Khan, D. A. (2019). Comparison of Nikto and Uniscan for measuring URL vulnerability. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), (pp. 1–6).
6. Lara, A., Kolasani, A., & Ramamurthy, B. (2013). Network innovation using openflow: A survey. IEEE communications surveys & tutorials, 16, 493–512.
7. Song, H. (2013). Protocol-oblivious forwarding: Unleash the power of SDN through a future-proof forwarding plane. Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, (pp. 127–132).
8. Wang, Y., & Yang, J. (2017). Ethical hacking and network defense: choose your best network vulnerability scanning tool. 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), (pp. 110–113).
9. Yang, L., Dantu, R., Anderson, T., & Gopal, R. (2004). Forwarding and control element separation (ForCES) framework. Tech. rep.
10. Yu, J., & Al Ajarmeh, I. (2010). An empirical study of the NETCONF protocol. 2010 Sixth International Conference on Networking and Services, (pp. 253–258).

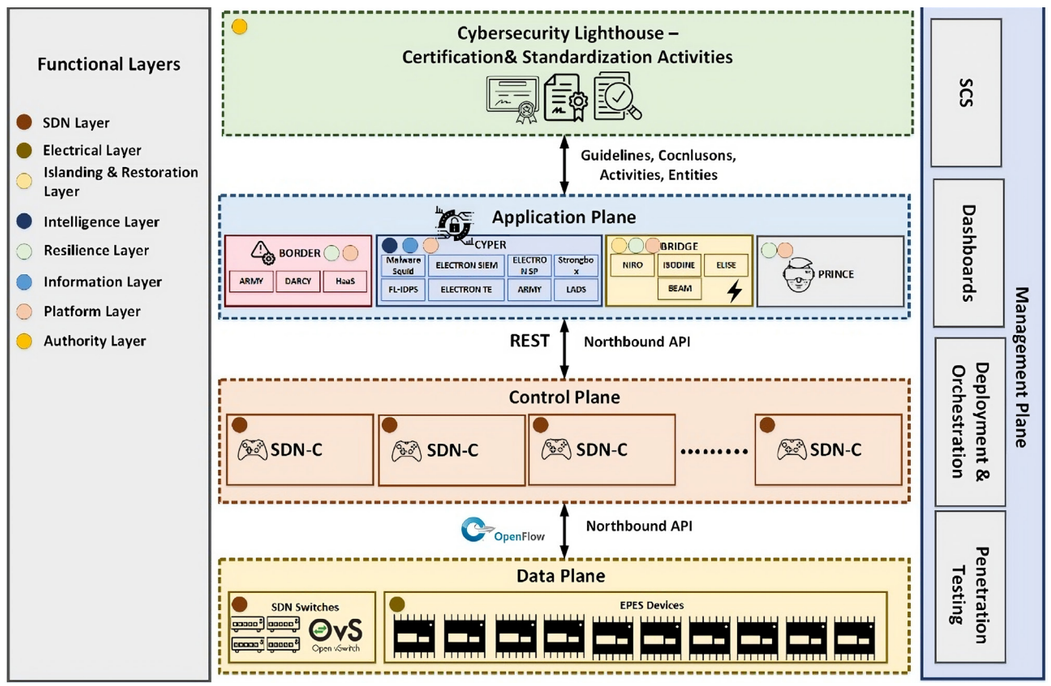


Figure 1: Conceptual View of the ELECTRON Architecture

ENCRYPT:

Revolutionizing Data Privacy: Innovations and Applications of the ENCRYPT Project

Stelios Erotokritou[1], Ioannis Giannoulakis[1], Emmanouil Kafetzakis[1]

[1] **Eight Bells Ltd**, Nicosia, Cyprus

Keywords

Data Privacy, Privacy-Preserving Technologies (PPTs), Cyber Threat Intelligence (CTI), Secure Data Processing

Extended Abstract

The increasing reliance on data-driven innovation across sectors such as healthcare, finance and cybersecurity has led to an increase in privacy concerns and the need for data protection frameworks. The ENCRYPT project, funded under the Horizon Europe Framework Programme, seeks to address these challenges by developing scalable, user-centric Privacy-Preserving Technologies (PPTs). This extended abstract provides an overview of the project's key innovations, including Fully Homomorphic Encryption (FHE), Trusted Execution Environments (TEEs), Differential Privacy (DP), hybrid solutions, and their user case applications. These technologies ensure compliance with regulatory frameworks like GDPR, offering enhanced security without sacrificing the utility or efficiency of data processing.

Introduction

Data is a critical asset in the modern digital landscape, driving innovation across various industries. However, with the growing volume and complexity of data, ensuring privacy during processing and data analysis has become increasingly challenging. Regulations like GDPR mandate data privacy protections, adding complexity for organizations that must comply while maintaining operational efficiency.

PPTs offer a solution by allowing data processing without exposing sensitive information. Despite this, they face limitations, including scalability and usability, which hinder their widespread adoption. The ENCRYPT project aims to overcome these barriers by advancing PPTs that are scalable, adaptable to the needs of various sectors and accessible to users from various fields and expertise.

Project Overview

The ENCRYPT project is focuses on developing innovative solutions to protect sensitive data across different sectors, including finance, healthcare and cybersecurity. ENCRYPT's primary objective is to revolutionize how data is processed and secured, ensuring compliance with GDPR and other regulatory frameworks. The project adopts a user-centric approach to ensure the technologies are accessible to users with varying levels of technical expertise.

ENCRYPT's core technologies include:

- **Fully Homomorphic Encryption (FHE):** Allows computations on encrypted data without decryption, ensuring data confidentiality during processing.
- **Trusted Execution Environments (TEEs):** Provides secure zones within processors to protect sensitive data during operations.
- **Differential Privacy (DP):** Introduces controlled noise into datasets, ensuring individual data privacy while maintaining the utility of the data.

Key Innovations

ENCRYPT's platform integrates these core technologies into a single, scalable solution, with an AI-powered recommendation system to assist users in selecting the most appropriate PPTs based on the type of data and its context. This user-friendly approach is key to ensuring the platform's widespread adoption across various industries.

Additionally, ENCRYPT addresses the computational challenges associated with PPTs through hardware acceleration, improving the performance of cryptographic operations like FHE. This enables the platform to process large datasets efficiently, making it practical for real-world applications in healthcare, finance, and cybersecurity.

Applications and Impact

ENCRYPT's technologies are designed for sector-specific applications:

- **Healthcare:** FHE and DP protect patient data during clinical research, enabling secure collaboration across institutions without compromising data privacy.
- **Finance:** DP, FHE and TEEs safeguard sensitive financial transactions, enhancing operational efficiency while ensuring regulatory compliance.
- **Cybersecurity:** TEEs secure the analysis and sharing of cyber threat intelligence, balancing the need for collaboration with stringent privacy protections.

Conclusion

The ENCRYPT project represents a significant advancement in the field of data privacy, offering solutions that are both technically advanced and practical for real-world use. By integrating multiple PPTs into a single, scalable platform, ENCRYPT enables secure data processing while maintaining compliance with privacy regulations like GDPR. The project's user-centric design ensures accessibility, making privacy-preserving technologies available to a broader range of users. Through continued innovation and collaboration, ENCRYPT aims to shape future standards in data privacy and security.

Acknowledgements

This work has been funded by the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No. 101070670 (ENCRYPT)

References

1. ENCRYPT Homepage, https://encrypt-project.eu/, last accessed 27/09/2024.
2. d'Antonio, S., Lazarou, G., Mazzeo, G., Stan, O., Zuber, M. and Tsavdaridis, I., 2023, July. The Alliance of HE and TEE to Enhance their Performance and Security. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 641-647). IEEE.
3. S.Erotokritou et al, "Revolutionizing Data Privacy: The ENCRYPT Project's Innovations and Applications", 21st European Mediterranean & Middle Eastern Conference on Information Systems, Athens, Greece, 2024.
4. Coppolino, L., D'Antonio, S., Mazzeo, G., Romano, L., & Sgaglione, L. (2022). PriSIEM: Enabling privacypreserving Managed Security Services. Journal of Network and Computer Applications, 203, 103397.
5. Jämes Ménétrey, Marcelo Pasin, Pascal Felber, Valerio Schiavoni, Giovanni Mazzeo, Arne Hollum, and Darshan Vaydia. 2023. A Comprehensive Trusted Runtime for WebAssembly with Intel

SGX. IEEE Transactions on Dependable and Secure Computing (2023). biometric data sharing can be regulated by strict data usage policies for sovereign data usage and control.

06. AI for Security

AP4AI:

A hands-on tool to assess accountability of AI applications

Babak Akhgar[1], Petra Saskia Bayerl[1]

[1] **CENTRIC,** United Kingdom

Keywords

Artificial Intelligence, Accountability, AI Assessment, Law Enforcement Agencies, AP4AI, Self-Assessment, EU AI Act Compliance, Risk Management

Extended Abstract

This paper outlines the concept and design of the AP4AI Assessment Tool. The tool is being co-designed with Law Enforcement Agencies (LEAs). The application of AP4AI for assessment of AI based tools will be discussed. The paper will address the notion of accountability in AI particularly in context of Justice and Home Affairs (JHA). The need for accountability in the application of Artificial Intelligence (AI) is widely acknowledged. The recently adopted EU AI Act explicitly references accountability as core requirement for implementation of AI within EU. The requirement for accountability is equally established in other international and national efforts, such as the UN and UK government, where the concept is named as a core principle for responsible AI (UK Government 2023). Notwithstanding its importance, the assessment of accountability is challenging. We describe AP4AI as a concrete effort to support LEAs' AI capabilities in context of assessing and evidencing AI accountability. The AP4AI tool was developed in the context of AI applications in the law enforcement, policing and security domain. Hence, we will illustrate the tool and its application on examples from this field using CODEV cycles of EU funded STARLIGHT project as a case study.

AP4AI tool was developed as part of the AP4AI (Accountability Principles for AI) Project (Akhgar et al., 2022). Its purpose is to provide a self-assessment tool for EU AI Act compliance as well as assess and evidence the accountability of specific LEAs' AI capability (e.g. image processing).

End-users can self-assess their conformity with EU AI Act and AI Accountability using a structured entry format, create reports to illustrate AI Accountability areas that are fully, partially or not (yet) addressed and receive recommendations how to rectify shortcomings. The reports can be used to evidence AI Accountability and provide a detailed account of the steps, procedures and mechanisms with which AI Accountability is achieved for accountability bodies within and outside the organisation. An additional objective of the tool is that, through the process of self-assessment, organisations and staff within organisations become increasingly knowledgeable about AI Accountability, facilitating organisational learning and longer-term leading to the integration of AI Accountability into organisational procedures and cultures.

Acknowledgements

The STARLIGHT (Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats) has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 101021797. https://www.starlight-h2020.eu/about

References

1. Akhgar et al. (2022). AP4AI Framework
2. Blueprint. AP4AI Report. Access online: www.ap4ai.eu
3. UK Government. (March 2023). A pro-innovation approach to AI regulation. White Paper Department for Science, Innovation and Technology. Available online: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach

STARLIGHT:

The STARLIGHT approach for AI research for Law Enforcement: capitalize on the past, build the present and anticipate the future

Nizar Touleimat[1]

[1] **CEA, LIST, 91191 Gif-sur-Yvette Cedex,** France

Keywords

AI, Law Enforcement, Technological sovereignty, Technological Autonomy, Cooperation, FCT

Extended Abstract

The STARLIGHT [1] project, is a 4-year project funded by the European Commission (EC). STARLIGHT is coordinated by CEA and brings together 50 partners representing 18 European countries, including EUROPOL and 14 law enforcement agencies (LEAs). The aim of the STARLIGHT project is to foster a community that brings together Law Enforcement, Researcher, Industry, and practitioners, actors if you will, in the security ecosystem under a coordinated and strategic effort to bring AI as a capability into operational environments of LEAs and incompliance with the EU AI Act. For the last 3 years, the partners have worked to extend a sustainable and multidisciplinary community, to build a coherent methodology and a strategic environment to provide European LEAs with interoperable and reliable AI solutions. The approach applied so far upholds EU legal, ethical and societal values whilst addressing high-priority threats in Europe.

In this paper we will address how Starlight project deployment methodology can 1) inspire the development of future research work programmes in security, 2) be used as an example of best practices for innovation projects and 3) that it could contribute to the European debate on the ethical and legal framework governing AI for security.

Adopt best practices and capitalize on the results already produced by other projects

In order to produce mature solutions (TRL7-8) that meet specific functional needs, STARLIGHT has, from its inception, taken into account the already existing EU and national projects in the field of AI for law enforcement. Thus, the project started by taking the best out of the already existing AI based technologies, datasets and solutions in the security dimension. The project has largely adopted the best practices developed by the ASGARD[2] project, such as the implementation of short technological development cycles, allowing quick and effective response to operational needs and the progress of the STARLIGHT research programme. STARLIGHT has also been built upon and improved the ASGARD hackathon approach, which brought together technology providers and LEAs within the same teams to better adapt developments to operational needs and constraints and ensure good adoption of the solutions developed by end-users. From the design of the project proposal, we carried out a significant amount of work mapping related projects and initiatives (GRACE[3], LAGO[4], etc.) to avoid reproducing existing solutions and to identify already mature technological building blocks and adequate data sets from which to build our solutions. Thus, STARLIGHT was able, from its launch, to begin to respond effectively to the needs of LEAs by optimising the use of its material resources and the time of the consortium members.

An adaptive LEA-centric co-development approach

STARLIGHT has also developed its own deployment methodology. The STARLIGHT methodology is based on a precise sequence of steps to collect the needs of the LEAs for operational functionalities, to identify and present to the LEAs technological capabilities based on AI that can meet their needs and to create teams including LEAs and developers working together on the co-development of very specific AI-based solutions by consideration for privacy and security by design in every step of its co-creation. Finally, all the solutions developed are tested and evaluated during pilots taking into account the different operational use cases prioritised by the LEAs. The STARLIGHT's approach based on successive cycles of co-developments running in parallel allows the consortium to address any eventual new threats identified by the LEAs and allows the adoption or adaptation of any new innovative technology.

A large, multidisciplinary and sustainable security research community

The STARLIGHT consortium was built to select the best and most relevant European partners to meet the project objectives. The consortium was also developed to national clusters consisting of, for example, an LEA and its trusted partners, to work in complete transparency and confidentiality when necessary. Obviously, most of the interactions are carried out via cross-border collaborations and this was made possible thanks to a history of collaborations already existing within a community that STARLIGHT is expanding.

Anticipating and implementing the European Ethical and Legal Framework

The STARLIGHT Ethical and Legal compliance assessment and monitoring approach relies on both internal structure and expertise and on external contributions and independent support.

The project internal approach is based on 4 pillars:

1. Legal and ethical assessments of all data used in the project with a precise and formalised assessment procedure facilitating data management and ensuring completeness checking and traceability
2. Bias detection and analysis of potential misuse in the context of bias, with the elaboration of recommendations for mitigation/minimisation of potential algorithmics bias
3. AI Act compliance: although the AI Act did not enter into force until the 1st of August 2024. STARLIGHT anticipated the discussion, debate and evolution of this legislation to prepare its AI development activities to strive for compliance with the Act.
4. Continuous internal support concerning legal and ethics compliance of STARLIGHT with 1) Direct interaction with technical activities 2) participation in co-development cycles, 3) wider guidance to all partners, 4) organisation of an ethical and legal observatory (ELO) and finally, 5) Collaboration with AP4AI[5] and sibling projects.

[1] www.starlight-h2020.eu
[2] www.asgard-project.eu
[3] www.grace-fct.eu
[4] https://lago-europe.eu/

Acknowledgements

This work is funded by the EU's H2020 research and innovation program under Grant No. 101021797.

[5] www.ap4ai.eu

07. Strengthened Security Research and Innovation

ENACT:

European Network Against Crime and Terrorism

André Alegria[1], Helen Gibson[2], Marialuna De Tommaso[3], Dorothea Tsatsou[4], Andreas Kosmatopoulos[4], Guillaume Brumter[5], Inês Cunha[6], Isabela Maria Rosal[7], Cyril Piotrowicz[8], Rocío Carbayo[9], Peter van de Crommert[10], Jarmo Puustinen[11], David Ríos Morentin[12]

[1] **Polícia Judiciária,** Portugal,

[2] **Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research,** United Kingdom,

[3] **Engineering,** Italy,

[4] **Centre for Research and Technology Hellas,** Greece,

[5] **European Organisation for Security,** Belgium,

[6] **Instituto de Engenharia de Sistemas e Computadores Inovação,** Portugal,

[7] **CiTiP – imec - KU Leuven,** Belgium,

[8] **Ministère de l'Intérieur,** France,

[9] **Ministerio del Interior,** Spain,

[10] **Politie,** Netherlands,

[11] **Sisäministeriö,** Finland,

[12] **Vicomtech,** Spain

Keywords

Knowledge Network, Fight against Crime and Terrorism, Research & Innovation, EU, Security

Extended Abstract

Introduction

ENACT (European Network Against Crime and Terrorism) is a Horizon Europe project aiming to enhance security research and innovation (R&I) in the fight against crime and terrorism (FCT) domain (European Network Against Crime and Terrorism, 2024). Launched in September 2023, the project runs for 36 months and seeks to consolidate knowledge, build networks and facilitate intra-stakeholder collaboration to support decision-makers, improve security practices, and foster the uptake of innovative solutions across the EU.

Objectives

The ENACT project has two primary goals: (1) providing evidence-based support to decision-makers in the FCT R&I ecosystem, thereby improving the programming of EU-funded security initiatives; and (2) acting as a catalyst for the adoption of cutting-edge security solutions. These objectives are pursued through a structured knowledge base and a structured knowledge network, involving collaboration between various internal knowledge observatories and external stakeholders in the FCT domain.

Methodology

ENACT employs a comprehensive and structured methodology through knowledge aggregation, analysis, and dissemination. This methodology is built upon four key pillars: Networking, Research, Communication, Dissemination and Exploitation (CDE), and Cooperation. Each pillar serves a distinct purpose, ensuring a holistic approach to addressing the evolving challenges in the FCT R&I domain.

ENACT's **Networking Pillar** establishes connections within the broader FCT community by identifying and registering key stakeholders from diverse sectors. This systematic stakeholder identification is (ENACT, 2024)achieved through active monitoring and participation in key industry events focused on security and technology. Networking ensures that the project taps into existing expertise while building partnerships to enhance cooperation.

The **Research Pillar** consists of four key observatories: Capabilities, Technology, Market, and Ethical, Legal & Societal (ELS), with an additional observatory acting as an Inter-Observatory Coordinator (IOC). These observatories systematically collect, analyse and categorise data using different relevant categorisation schemata, but most prominently the FCT-pertinent aspects of the EU civil security (EUCS) taxonomy (European Comission: Directorate-General for Migration and Home Affairs, 2022) of the EU Civil Security framework (European Commission: Directorate-General for Migration and Home Affairs, 2022). Key outputs of this pillar include periodic reports, flash reports, advanced analytical assessments and a populated structured knowledge base (SKB) of observations that have been aggregated to (a) feed the reports after appropriate analysis, (b) be made available to FCT stakeholders (public vs private dissemination considered).

The **Communication, Dissemination, and Exploitation (CDE) Pillar** is crucial to ENACT's ability to transform knowledge into actionable insights for the FCT R&I community. This pillar ensures that the wealth of information collected through ENACT's observatories and stakeholder engagement is effectively communicated, widely disseminated, and exploited for its full potential.

Finally, the **Cooperation Pillar** fosters collaboration and partnership among a diverse range of stakeholders in the FCT R&I domain, providing financial support to third parties. ENACT relies heavily on its network of stakeholders, including private companies, public bodies, academic institutions, and research centres. By actively engaging stakeholders and supporting initiatives such as relevant events, research project's demonstrations, and promising results already identified by DG HOME, ENACT fosters collaboration, knowledge sharing, and the uptake of novel solutions, thus promoting innovation and alignment with EU security priorities.

Results

During its first year ENACT delivered several key products to the FCT community:

- FCT R&I Stakeholder Map: ENACT identified over 1,000 stakeholders across 52 countries, creating a robust network of actors involved in FCT security initiatives (ENACT, 2024). This map will continue to evolve as the project progresses.
- FCT Capability, Technology, Market, and ELS Maps: ENACT produced detailed maps for each observatory, outlining the state of FCT research (ENACT, 2024), technologies (ENACT, 2024), market trends (ENACT, 2024), and legal and societal considerations (ENACT, 2024). These maps consolidated data from 671 observations across news, projects, scientific materials and policy papers.
- Flash, Advanced and State-of-Play Knowledge Reports: ENACT produced several reports focused on security research trends (ENACT, 2024) and market overviews (ENACT, 2024) (ENACT, 2024), based on a set of over 550 observations aggregated in its SKB. These reports offered targeted insights to support decision-making in the security domain. A State-of-Play Policy report was also released (ENACT, 2024), summarizing the outcomes of the Observatories' work.

In addition to these, ENACT has already established multiple Memorandi of Understanding with the 2023 winners of the Security Innovation Awards promoted by DG HOME to support them in further

disseminating and exploiting their solutions to reach a wider range of the FCT R&I community.

The project ended its first year by organising an annual event open to the community, with the aim of showcasing the results obtained so far, highlighting the opportunities for collaboration with FCT projects and stakeholders and the key project outputs - designed for the benefit of the whole FCT community. Two insightful roundtable discussions also took place, comprising of a panel of FCT experts from LEAs, Policy, Industry and Research, who came together to discuss the role for knowledge networks in research and innovation community and mechanisms for enhancing collaboration within FCT. The event saw an attendance of 123 participants. Attendees represented a diverse mix of organisations, providing excellent representation from across the FCT community - 11% were from organisations relating to policy, 16% from industry, 23% from research and technology, 37% from law enforcement agencies, and 14% from other parts of the research and innovation community.

Impact

ENACT's knowledge network is poised to significantly enhance the EU's capabilities in addressing FCT challenges. By fostering collaboration between diverse stakeholders and promoting innovative security solutions, the project supports both immediate and long-term security goals. Its systematic approach to data collection and dissemination ensures that the insights derived from the project are grounded in empirical evidence, thus contributing to more effective policymaking and innovation uptake.

Conclusion

ENACT is playing a crucial role in advancing the EU's security landscape by facilitating knowledge exchange and fostering innovation. Its multi-observatory approach and strong stakeholder engagement have positioned the project as a key enabler of enhanced FCT capabilities and strategies. As the project progresses, ENACT is expected to continue generating impactful products that will help EU law enforcement agencies, policymakers, and researchers to better address the evolving threats in the security domain.

Acknowledgements

Funded by the European Union Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

1. ENACT. (2024). ENACT 2024 FCT Maps -Capabilities Observatory. Retrieved from https://enact-eu.net/wp-content/uploads/2024/10/2024-FCT-Map-CapO.pdf
2. ENACT. (2024). ENACT 2024 FCT Maps-Ethical, Legal and Societal Observatory. Retrieved from https://enact-eu.net/wp-content/uploads/2024/10/2024-FCT-Map-ELSO.pdf
3. ENACT. (2024). ENACT 2024 FCT Maps-Markets and Standards Observatory. Retrieved from ENACT 2024 FCT Maps-Markets and Standards Observatory
4. ENACT. (2024). ENACT 2024 FCT Maps-Technology Observatory. Retrieved from https://enact-eu.net/wp-content/uploads/2024/10/2024-FCT-Map-TechO.pdf
5. ENACT. (2024). ENACT 2024 FCT State of Play Policy Report. Retrieved from https://enact-eu.net/wp-content/uploads/2024/10/SoP-Report-2024-Digital-version.pdf
6. ENACT. (2024). ENACT FCT Stakeholder Map. Retrieved from ENACT Website: https://enact-eu.net/enact-fct-stakeholder-map/
7. ENACT. (2024). FCT R&I: An analysis of EU priorities 2014- 2024. Retrieved from https://enact-eu.net/wp-content/uploads/2024/04/ENACT-Analytical-Report-01-FCT-RI-An-analysis-of-EU-priorities-2014-2024.pdf
8. ENACT. (2024). Security Market Overview: TECNOSEC & DRONExpo Event. Retrieved from https://enact-eu.net/wp-content/uploads/2024/07/ENACT-FLASH-REPORT-2-TECNOSEC-EVENT.pdf
9. ENACT. (2024). Security Market Overview: Trends & Insights from the SICUR Exhibition. Retrieved from https://enact-eu.net/wp-content/uploads/2024/04/ENACT-FLASH-REPORT-1-SICUR-exhibition.pdf
10. European Comission: Directorate-General for Migration and Home Affairs. (2022). EU civil security taxonomy and taxonomy explorer. Retrieved from https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-taxonomy-and-taxonomy-explorer_en
11. European Commission: Directorate-General for Migration and Home Affairs. (2022). EU security market study: final report. Publications Office of the European Union.
12. European Network Against Crime and Terrorism. (2024, October 2). Retrieved from CORDIS - EU research results: https://cordis.europa.eu/project/id/101121152

MultiRATE:

Holistic framework for the MatUrity evaLuaTIon of ReAdiness level for security TEchnologies

Antonia Kardara[1], Eleni Darra[1], Luis Unzueta[2], Hoog Bjorne[5], Goncalo Cadete[6], Salvatore Vicari[7], Alexei Grinbaum[8], Sirra Toivonen[3], Marcel van der Lee[4], Souzana Sofou[9], Dimitrios Diagourtas[9], Helen Gibson[12], Luke Bates[12], Michalis Angelou[1], Nikolaos Vrettos[1], Dimitrios Kavallieros[1], Babak Akhgar[12], Theodora Tsikrika[1], Stefanos Vrochidis[1]

[1] **ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS (CERTH),** Greece,

[2] **FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH (VICOM),** Spain,

[3] **TEKNOLOGIAN TUTKIMUSKESKUS VTT OY (VTT),** Finland,

[4] **NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO (TNO),** Netherlands,

[5] **FRAUNHOFER- GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG EV (Fraunhofer),** Germany,

[6] **INOV INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES INOVACAO (INOV),** Portugal,

[7] **ENGINEERING - INGEGNERIA INFORMATICA SPA (ENG),** Italy,

[8] **COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA),** France,

[9] **SATWAYS-OLOKLIROMENES LYSEIS ASFALEIAS KAI AMYNAS-IDIOTIKI EPICHEIRISI PAROCHIS YPIRESION ASFALEIAS (IEPYA)-ETAIREIA PERIORISMENIS EFTHYNIS (STWS),** Greece,

[10] **POLISMYNDIGHETEN SWEDISH POLICE AUTHORITY (SPA),** Sweden,

[11] **SERVICE DEPARTEMENTAL INCENDIE ET SECOURS SDIS (SDIS78),** France,

[12] **SHEFFIELD HALLAM UNIVERSITY (CENTRIC),** United Kingdom

Keywords

Readiness Level, Maturity, Validation, Holistic Readiness Level, Readiness Assessment

Extended Abstract

In recent years, numerous metrics have been developed to evaluate the maturity of products, systems, and processes, particularly regarding their deployment readiness. Despite substantial efforts to integrate widely used frameworks, methodologies, and indicators, the application of these tools within EU-funded security research and innovation (R&I) projects remains limited. This underlines the need for a comprehensive and consistent scaling framework. The MultiRATE framework addresses this gap by developing new (where needed), amending and integrating existing readiness level approaches into a single, robust, and reliable structure that evaluates all aspects of products, systems, and processes.

To develop this framework, MultiRATE conducts an in-depth analysis of current methodologies, creating a well-defined scale that incorporates several established readiness levels. The key readiness levels included in the MultiRATE framework are as follows:

- **Technology Readiness Level (TRL):** utilizes a plethora of indicators per RL based on four categories: (i) Technology Preparation &Requirements, (ii) Reporting Documents, (iii) Operability &Continuity (iv) Evaluation & Usability to evaluate the current level (1-9) of the technology under evaluation [3].
- **Societal Readiness Level (SocRL):** measures the take-up and acceptance of an innovation by society. Innovations are based on the results of new technological developments, technology combinations, or other knowledge towards societal well-being, and should be developed alongside stakeholder input to ensure they are suitable for their intended purpose and accepted within their context [1].
- **Security Readiness Level (SecRL):** offers a systematic, clear, and objective assessment of an element's readiness regarding its security. This particular security perspective enhances the understanding of the element's readiness to operate in contested or potentially hazardous environments.
- Legal, Privacy, and Ethics Readiness Level (LPERL): iteratively indicates (i.e. the tool should be used multiple times during development and results should be compared to each other) the ethical, privacy, and legal readiness of products/ outcomes, and raise awareness of potential current and downstream issues in the evaluated aspects.
- **Manufacturing Readiness Level (MRL):** supports the industrialisation manager sand R&D teams in managing manufacturing risk and ensuring the manufacturability of products in the transition from R&D to production. Potential investors of a new product can also benefit from having an accurate assessment of its manufacturing readiness level [2].
- **Commercialisation Readiness Level (CRL):** supports an exploitation team in assessing their product's readiness for the market, and enrich the action plan to improve the product's commercialisation strategy and innovation adoption. Six indicator categories are being examined in a 9-step assessment process, and the indicators serve as guidelines to achieve the goal.
- **Integration Readiness Level (IRL):** intends to evaluate and quantify the maturity and readiness of an element (component, system, technology) for integration into a broader system or environment. It provides a framework for assessing technological capabilities, interoperability, standards, documentation, and other variables critical to effective integration.
- **Forecasting Module (FM):** intends to get the best possible prediction of how a specific funding, measured in person-months (PMs) – that we consider as a widely objective measure – will affect the increase of a proposed project with specific features in terms of the TRL (or any other RL) scale based on AI.

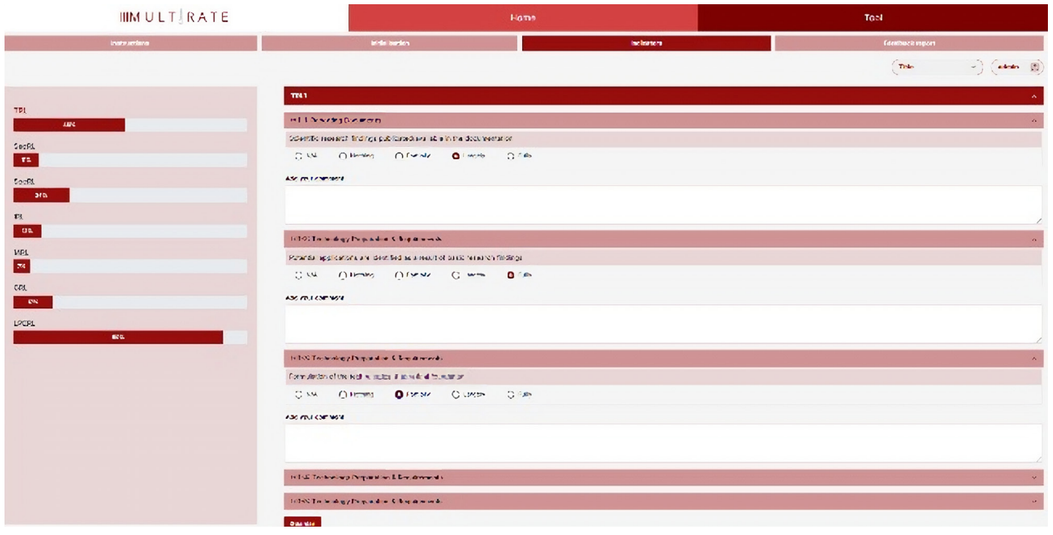
These readiness levels form the foundation of a comprehensive MultiRATE framework designed to evaluate the maturity of products, systems, and processes from multiple perspectives. More specifically, the MultiRATE **Holistic Readiness Level** (HRL) combines these elements into a cross-disciplinary methodology that will be made available to the EU R&D community.

Holistic Readiness Level

The HRL (Figure 1) has been evaluated based on user needs, with regular updates implemented based on testing and feedback from the MultiRATE network. Feedback regarding the HRL, in conjunction with insights from other RL scales, was utilized to inform ongoing improvements to for subsequent evaluation rounds. Initial feedback from evaluators was varied; while the current HRL was considered largely

effective by some, significant refinement was deemed necessary by others. Common suggestions for improvement included enhancing content, providing additional guidance, and improving interface design, all of which were aimed at strengthening the overall evaluation process of the HRL. The graphical interface has been updated according to the input received (Figure 1) to better present for example the indicators and the results of an assessment.

Furthermore, evaluators suggested presenting all indicators in a vertical list to allow non-sequential answering and increasing the font size of indicator descriptions for better visibility. The inclusion of a "Non-applicable" option, tick boxes for completed indicators, and clearer levels with completion percentages for each RL was also recommended. Feedback varied, with some evaluators finding it unclear, while others felt it largely met its goals. Thus, suggested enhancements have been taken under consideration and have been implemented to strengthen the overall experience of the users.



Acknowledgements

Funded by the European Union. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or REA. Neither the European Union nor the granting authority can be held responsible for them.

References

1. Büscher, M., Cronshaw, C., Kirkbride, A., Spurling, N. Making Response-Ability: Societal Readiness Assessment for Sustainability Governance. Sustainability 2023, 15, 5140. https://doi.org/10.3390/su15065140
2. United States Department of Defence, Manufacturing Readiness Levels Definitions, last visited April 2024
3. I. Bruno, G. Lobo, B. V. Covino, A. Donarelli, V. Marchetti and A. S. M. F. Panni, "Technology readiness revisited: a proposal for extending the scope of impact assessment of European public services," ICEGOV, pp. 369-380, 2020.

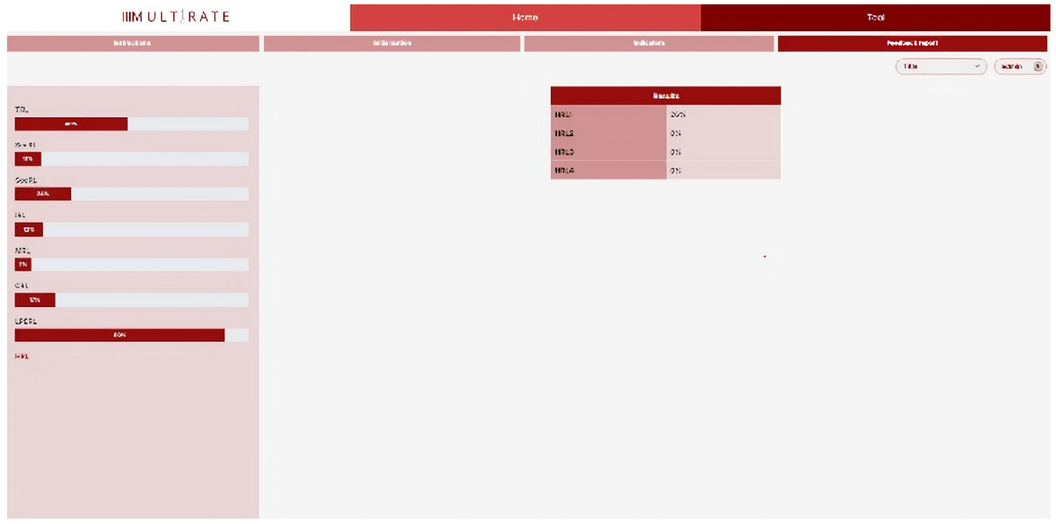


Figure 1: HRL Indicators and Results

08. Networks of Security Practitioners

CYCLOPES:

Cybercrime Law Enforcement Practitioners' Network

Steven Ormston

Polish Platform for Homeland Security

Keywords
Cybercrime, Cyber-enabled Crime, Practitioner Network

Extended Abstract

The CYCLOPES project, officially known as the Cybercrime Law Enforcement Practitioners' Network, is an EU-funded initiative established to combat the escalating threat of cybercrime. Launched in May 2021, the project is set to run until April 2026, with a total budget of approximately €3.5 million under the Horizon 2020 programme.

The CYCLOPES project (Cybercrime Law Enforcement Practitioners Network) is an EU-funded initiative dedicated to enhancing the fight against cybercrime through the establishment of a robust network among law enforcement agencies (LEAs) across Europe. Launched in May 2021, this five-year project will run until April 2026, with funding of approximately €3.5 million from the Horizon 2020 programme.

The Polish Platform for Homeland Security (PPHS) coordinates the project and plays a pivotal role in managing its activities and ensuring effective collaboration among its partners.

The CYCLOPES consortium initiated the initiative in response to the rapidly increasing and complex nature of cybercrime, which poses significant public safety and security threats. The impact of cyber-related crime in Europe is enormous, underscoring the need for additional responses from law enforcement and the research community.

A project to build and maintain an innovation-driven network of LEAs combating cybercrime - accelerating the EU's ability to counteract growing pressures of cyber threats. Heeding advice from EUROPOL's EC3 flagship report Internet Organised Crime Threat Assessment, CYCLOPES create synergies between LEAs from MS and connect industry and academia by stimulating and sustaining dialogue on pressing security matters threatening the stability of Europe and Citizen safety.

A critical component of the project involves conducting practitioners' workshops that focus on various aspects of cybercrime, including mobile device forensics, social engineering, and the challenges posed by cryptocurrencies. The Practitioners' workshops are a driving force and cover three 3 domains: 1) cybercrime affecting people directly, 2) cybercrime affecting systems, 3) digital forensics – a horizontal topic for the network.

Based on the gaps and needs highlighted, the team reviews the research and commercial markets, identifying solutions and innovation activities to highlight actions and novel products to assist LEAs tackle the complexity of cybercrime.

Besides technology, the project supports the continued development of LEAs, working closely with practitioners to define current capacities and elicit capability gaps and requirements in crucial areas: procedures, training, legal and standardisation. Consequently, other objectives are: identification of priorities for standardisation; recommendations for innovation uptake and implementation; social, ethical and legal reports providing guidance and training suggestions for cybercrime investigators; dissemination of results through workshops, conferences, webinars, publications, policy papers and media. All outcomes will be suitably considered for exploitation - helping to propel the EU in the fight against cybercrime.

The project synchronises with other activities conducted by relevant parties EUROPOL, INTERPOL, CEPOL, ECTEG, EACTDA, ENISA; networks: ENLETS, ENFSI, I-LEAD, iLEAnet, EU-HYBNET, covering topics that go beyond efforts of these initiatives and preventing duplication. This also applies to projects where activities align with CYCLOPES (i-ProcureNet, Stairs4Security) and future projects funded by the EC, especially in the area of AI.

By identifying capability gaps and specific requirements of practitioners, CYCLOPES aims to bolster the capacity of law enforcement to combat evolving cyber threats effectively.

The project delivers value primarily to law enforcement agencies and extends to academia and the private sector, including small and medium-sized enterprises (SMEs). By fostering dialogue and collaboration among these stakeholders, CYCLOPES enhances the collective ability to tackle cybercrime through shared knowledge, resources, and best practices.

In summary, the CYCLOPES project is a useful initiative to strengthen law enforcement's capabilities across Europe in the face of growing cyber threats. Through its collaborative network, commitment to innovation, and focus on best practices, CYCLOPES seeks to foster a safer digital environment for all citizens and to contribute to the existing ecosystem.

For more detailed information, you can visit the official CYCLOPES project website (www.cyclopes-project.eu).

NOTIONES:

Interacting network of intelligence and security practitioners with industry and academia actors

Yantsislav Yanakiev[1]

[1] **Bulgarian Defence Institute "Professor Tsvetan Lazarov,** Bulgaria

Keywords

Security Practitioners, Intelligence, Counterterrorism, Intelligence Cycle, Technologies for Intelligence

Extended Abstract

NOTIONES is a Latin lemma meaning "notions, ideas, investigations, and cognisance" and therefore refers to "being informed".

The objectives of NOTIONES are:

- To identify the intelligence and security practitioners' needs in order to focus the research and development efforts on their needs and requirements with respect to emerging and disruptive technologies and organisational processes.
- To promote interaction of technology providers and academy with the intelligence and security practitioners by matching the practitioners' requirements with existing or upcoming technological solutions.
- To find out new technologies relevant for practitioners.
- To periodically publish a report which summaries findings in order to orientate future research project programming.
- To ensure the commitment and involvement of new organizations in the pan European NOTIONES network.

The NOTIONES consortium includes:

1. 15 practitioners from military, civil, financial, judiciary, local, national and international polices, coming from 9 EU MS and 6 AC. These practitioners, together with the other consortium members, grant a complete coverage of the 4 EU main areas: Western Europe (PT, ES, UK, FR, IT, DE, AT), North Europe (FI, DK, SE, EE, LV), Middle Europe (PO, SK, UK), Middle East (IL, TR, GE, BG, BA, MK) for a total of 21 countries;
2. experts in security research programming.

The monitoring of technologies and the definition of requirements and recommendations for their industrialization is expected to provide a great advantage to practitioners in the fields of intelligence and security. Through an iterative cycle, the output recommendations will be synthesized into specifications that can be provided to industry and academy across Europe, providing tangible benefits to those organisations engaged in intelligence and security.

The results of the NOTIONES project, which has a lifetime of five years, have been presented to the broad intelligence community in workshops and conferences and will contribute to the definition of further security and intelligence research.

Work Packages:

- WP1 – Project coordination and management
- WP2 – Intelligence process and preliminary requirements - BDI Lead
- WP3 – Technologies for intelligence
- WP4 – Terrorist process
- WP5 – Monitoring of innovation
- WP6 – Interaction between practitioners and other stakeholders
- WP7 – Workshops and conferences
- WP8 – Dissemination, communication and exploitation activities

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021853.

09. European Defence Technologies

ACTING:

Advanced European platform and network of Cybersecurity training and exercises centres (ACTING)

Yantsislav Yanakiev[1], Eleni Darra[2], Dimitrios Kavallieros[2], Theodora Tsikrika[2], Stefanos Vrochidis[2]

[1] **Bulgarian Defence Institute "Professor Tsvetan Lazarov",** Bulgaria,

[2] **The Centre for Research and Technology Hellas,** Greece

Keywords

Cyber Security, Cyber Training, Cyber Exercise, Situation Awareness, Cyber Ranges, Cyber Defence

Extended Abstract

The goal of the ACTING project is to deliver an organized and coordinated approach to proactively improve efficiency of cyber defence training and exercises, through effective and efficient multi-sector collaboration.

To achieve this, ACTING conducts research and develops tools in the following five main areas:

- **Simulated user method and technology**- software agents deployed in cyber range scenarios, simulating user behaviour;
- **Automated performance analysis**- application that collects data about the activities of cyber trainees within the scenarios, provides measurements and performance analysis (visual and numerical), as well as identifies directions for training improvement that needs to be performed for a specific user;
- **Scenario Development Language**- metalanguage capable to translate cyber range scenarios developed by consortium or external partners to be integrated and understandable for other cyber ranges as well as for human beings;
- **Multi-domain simulations** (Federated Cyber Ranges)-Extending and improving existing federation of cyber ranges and developing common standards, interfaces and APIs for federation and information exchange;
- **Situational awareness and scoring**- elements covering perception, cognition and projection elements of the Situation awareness for the cyber domain under the umbrella of common information exchange protocols and standards working in federated environment and addressing cognitive aspects as well.

The aforementioned R&D activities will be demonstrated and validated under three scenarios:

Scenario 1: Combined cyberattacks against joint HQ, Land and Navy CIS systems

- Multi-domain cyber range simulation of cybersecurity attacks on common HQ cis for planning, Land and Navy CIS for Common Recognized Picture /CRP/ data exchange and its impact on planning, logistics, liaison with partners, high representatives daily/weekly schedule and discredit and reduce effectiveness

Scenario 2: Space and Maritime

- Multi-domain cyber range simulation of cybersecurity attacks on satellite and its impact on positioning, navigation, and timing systems

Scenario 3: Cascading effect for cyber-attack in civilian sector (telecom and land or navy)

- Multi-domain cyber range simulation of cybersecurity attacks on IoT and its impact on security environment by the breakthrough of commercial networks and obtaining PHI/PII information.

Acknowledgements

Co-funded by the European Union

Funded by the European Union (EDF-2021-CYBER-D-IECTE-2; Project Number: 101103208). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

CASSATA:

CASSATA – Covert and Advanced multi-modal Sensor Systems for tArget acquisiTion and reconnAissance

Lazaros Karagiannidis, Alexandros Rammos, Thanasis Douklias, Eleftherios Ouzounoglou, Angelos Amditis[1]
Konstantinos Ioannidis[2]
CASSATA Consortium[3]

[1] **Institute of Communication and Computer Systems (ICCS),** Greece,

[2] **The Centre for Research and Technology Hellas,** Greece,

[3] **https://cassata-project.eu/**

Keywords

ISTAR Missions, Covert Sensing, Optronics, Acoustic/Seismic Sensors, RADAR

Extended Abstract

The global strategic and operational landscape in which European Armed Forces must deploy and respond is characterized by rapid changes and ongoing transformations [1]. This reality makes it imperative to continually update military capabilities [2]. New technologies, especially digital advancements, are reshaping the security and defence sectors at an unprecedented rate, impacting established power balances within the global security framework [3]. Therefore, it is crucial to ensure that Europe's security and defence sectors remain technologically proficient and fit for purpose. Today's missions of the European Union (EU) military forces face swiftly emerging challenges and highly adaptive threats from adversarial forces across all domains—air, sea, and land [4]. In response, there is a pressing need to adapt, enhance efficiency, and achieve greater effectiveness to be optimally prepared and to secure superiority. Achieving these objectives requires the introduction of innovative methods, concepts, and multi-sensor platforms for covert, enhanced, and reliable target sensing. It also necessitates improved battlefield situational awareness, advanced early warning systems, robust decision support, efficient action planning, and enhanced capabilities for executing operations [5].

CASSATA aims to foster and enable the digital transformation of the EU military armed forces by analysing and designing systems, solutions and integrated concepts that will enable superior operational and tactical level information gathering, evaluation processes and battlefield situational awareness in all domains (i.e., air, sea, land, joint) while being themselves difficult to detect, track and intercept. CASSATA provides improvements in a whole range of Covert Sensing (CS) domains. More specifically the activities of the project are organised into four (4) specific Technical Areas (TA) and Sub-TAs.

CASSATA implements innovative technologies to improve the covertness of optronics sensors as well as their capabilities of detection, tracking, classification and identification. In addition, CASSATA studies three types of acoustic/seismic sensors that contribute to the network of sensors providing coverage for previously undetectable targets in challenging environments. Moreover, CASSATA implements innovative technologies and/or upgrade current technologies to provide covert RF sensors or to improve their capabilities of detection and tracking for different types of targets. The use of data fusion and collaboration techniques, Artificial Intelligence, and Machine Learning is applied to maximize the ISTAR capabilities of the sensing systems themselves, as well as those of the multi-sensing platforms.

More specifically, the first TA is focused on "Optronics for covert sensing", where the improvements on the capabilities of the optronics systems have been divided into three topics: i) TA1.1: Active imaging and ranging sensors; ii) TA1.2: Passive imaging sensors; and iii) TA1.3: Non-visual sensors (chemical). The second TA tackles acoustics/seismic sensing and has been devised into three topics: i) TA2.1: Acoustic/seismic networks for area surveillance; ii) TA2.2: Micro Electro-Mechanical System (MEMS) based acoustic sensors; and TA2.3: Opto-acoustic sensors. The third TA envelops RF and RADAR systems for covert sensing and has been devised into four topics: i) TA3.1: New kinds of illuminators using new frequencies; ii) TA3.2: Improvement of the passive radar robustness versus the environment; iii) TA3.3: Improvement of the threat spectrum detected by passive radar and Radio Direction Finding systems; and iv) TA3.4: Design of covered multistatic sensor network. Finally, the fourth TA focuses on Adaptive and Collaborative Sensing, Data Processing, Fusion, AI, and Sensor Management. This TA addresses three topics: i) TA4.1: Sensor Management and Processing focuses on the management of the set of sensors; ii) TA4.2: Sensors Raw Data Exploitation, Fusion, and Interoperability involves the fusion of sensor data provided by sensors with different technologies and capabilities; and iii) TA4.3: Services for Collaborative Sensors.

The techniques, methodologies, and solutions designed within CASSATA will undergo testing and validation in suitable simulation and laboratory environments. This is conducted using a use-case-oriented approach that addresses dynamic and complex scenarios. For these four TAs, the project identifies and assesses disruptive capability opportunities based on covert sensing that could offer a strategic advantage in EU's defence. Ultimately, the project intends to propose and evaluate strategies for capability building and sustainability centred around CS Technologies for i) improved target detection, identification and tracking in multi-domain operations, ii) enhanced data processing, fusion and correlation capabilities of multi-sensor platforms, iii) flexible deployment and scalability options tailored to the specific mission's needs, iv) intelligent and autonomous cueing and interworking of sensing systems, v) reduced vulnerability of armed forces and platforms, vi) increased robustness against changes of the environment and the target characteristics.

The project aims to significantly enhance situational awareness by improving target acquisition and sensor fusion in complex environments. By enabling flexible deployment and scalability options for multi-domain and multi-mission operations, it effectively addresses new conflict scenarios and adapts to evolving threats. The development of intelligent cueing and interoperability between existing and new sensing systems and platforms reduces the probability of being detected by enemy forces. Furthermore, the project emphasizes robust multi-sensing techniques that can withstand changes in the environment and target characteristics, supporting multi-mission operations with increased reliability.

Acknowledgements

Funded by the European Union (EDF-2022-RA-CASSATA; Project Number: 101121447). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

1. European Union. (2016). Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. Brussels: European External Action Service. Retrieved from https://europa.eu/globalstrategy/en
2. European Defence Agency. (2018). Capability Development Plan (CDP) 2018. Brussels: EDA. Retrieved from https://eda.europa.eu/docs/default-source/eda-publications/eda-brochure-cdp-2018
3. Fiott, D. (2017). The Card on the EU's Defence Ambitions: The White Book and the Commission's Defence Fund. Brussels: EU Institute for Security Studies. Retrieved from https://www.iss.europa.eu/content/card-eu%E2%80%99s-defence-ambitions
4. European Commission. (2016). Implementation Plan on Security and Defence. Brussels: European Commission. from https://eeas.europa.eu/sites/default/files/eugs_implementation_plan_st14392.en16_0.pdf
5. Griffiths, H. D., & Baker, C. J. (2017). An Introduction to Passive Radar. Boston: Artech House.

CUIIS:
Comprehensive Underwater Intervention Information System

Sergey Belkinov

Bulgarian Defence Institut, Bulgaria

Keywords

Diving, Hyperbaric, Command and Control, Common Operational Picture, Underwater-Unmanned Vehicles, Underwater Communication, Decompression Sickness, Situational Awareness, Intelligent Diving Equipment

Extended Abstract

Development of innovative information system, providing comprehensive monitoring, communications, management and situational awareness at a lower tactical level, able to support the full spectrum of underwater intervention operations in expeditionary setting, both at sea and in inland bodies of water, as per the concept of the Deployable Modular Underwater Intervention Capability Package (DIVEPACK) PESCO Project[1].

Description of the concept (Figure 1)

The system provides uninterrupted real time monitoring of the physiological condition of a diver underwater, calculation of optimized decompression profile, taking into account the values of constantly registered relevant physiological parameters, and real time visualization of the outcome information, both for the diver underwater and for the diving supervisor on the surface. The system also determines the location of diver(s) underwater and visualize it for the diving supervisor on the surface, and it provides platform for manned-unmanned teaming, including when big number of divers and Unmanned Underwater Vehicles (UUVs) are being employed simultaneously.

The system includes the following components:

Component № 1: Component for real time monitoring, registering and data transmission of relevant physiological parameters of a working diver underwater (number and size of inert gas bubbles in the diver's blood, heart rate, ECG, body temperature, hydration, oxygenation.

The subject is designed as a diving suit with integrated sensors ("smart" diving suit). The embedded sensors monitor the values of particular relevant physiological parameters and transmit/send them for further registration and processing by the next component (Component № 2).

Component № 2: Component for real time automatic calculation of individualized decompression profile, taking into account the following variables as a minimum: individual body characteristics; current physiological parameters of the diver; age; the diving equipment being used and the chosen breathing gas/mixture; environmental factors etc.

The design of the component is an innovative diving computer (both as hardware and as software). The calculated/optimized decompression profile visualized real time, both for the diver underwater and for the diving supervisor on the surface.

Component № 3: Component for tracking and visualization (on the surface) of the

[1]https://pesco.europa.eu/project/deployable-modular-underwater-intervention-capability-package-divepack/

real time location of a diver working underwater.

This component also facilitates the necessary data/ information transmission/ flow between the three system components. It provides communications between the diving supervisor and the working diver(s), including when multiple divers and UUVs (AUVs, ROVs, etc.) are being employed simultaneously in a manned-unmanned teaming setting. The aim is to design this component as an innovative underwater information system, supporting the integration and joint operation of all the other components as one set.

Component № 4: Component for individualized automated surface decompression or emergency recompression.

The main goal is to have the subject component as an onsite portable (to include inflatable) hyperbaric chamber with automated electronic controls, capable to receive wireless the individual divers' information package from the diving supervisor's console, in order to prepare and execute, once activated, a suitable surface decompression/ emergency recompression profile.

The development of the system passed through the following stages: Feasibility study; Design development; Definition of Technical Specifications; Prototyping; Testing; Qualification and Certification for the separate components, as well as for the system as a whole.

Acknowledgements:

This project has received funding from the European Defence Industrial Development Programme under Grant Agreement EDIDP-UCCRS-EDD-2020-059 - CUIIS. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Comprehensive Underwater Intervention Information System Concept

Figure 1

FaRADAI:
Frugal and Robust AI for Defence Advanced Intelligence

Andromachi Papagianni[1], Konstantinos Ioannidis[1], Theodora Tsikrika[1], Stefanos Vrochidis[1], Ioannis Kompatsiaris[1]

[1] **Centre for Research and Technology Hellas**, 6th km Charilaou-Thermi Rd, P.O. Box 60361, Thermi, GR 57001 Thessaloniki, Greece

Keywords

Data Privacy, Privacy-Preserving Technologies (PPTs), Cyber Threat Intelligence (CTI), Secure Data Processing

Extended Abstract

AI technology has influenced significantly different aspects of modern society [1] and economy [2]. Recent technological advancements led to improved decision-making and support systems, as well as autonomous processes, by utilizing different types of data, such as text, sound, visual content, and video footage. A major concern when implementing AI models is that, to provide accurate outcomes, they require collection and preparation of a number of representative data that leads to a costly and timely process, in terms of hardware and human resources.

When referring to the defence domain [3], data may be characterized as limited or incomplete, as well as sensitive in nature, requiring security clearance for proper labelling by dedicated personnel. Another aspect of the domain that should be taken into consideration regards the strict safety and security regulations that need to be followed. When employing AI algorithms in military applications, it is essential that any recommendations and decisions made are compliant with the respective regulations, considering the complex and continuously changing environment. Furthermore, an AI framework must have a user-friendly interface and be interpretable from the perspective of operators such as commanders.

Following the specificities of using AI models in the defence domain, FaRADAI project aims to deliver new approaches, algorithms and tools, as research products, to address some of the most prominent issues relevant to AI applicability on a military environment and more specifically:

- Frugal AI: The deployment of an AI framework in modern warfare requires high levels of accuracy that are strongly linked with the existence of operation-specific data. However, there is limited availability of sufficient annotated data that may also be marked as sensitive, and could not be disclosed even within European Member States. In the same approach, essential data are relevant to specific types of sensors, with the available public datasets usually used not being appropriate to the operational requirements.
- Robustness and explainability: An operational-ready AI framework must remain reliable in case of natural or artificial perturbations (Robust AI). Furthermore, the guidelines of the framework must be trusted and understood to be acceptable by humans (Explainable AI). In the defence domain, the variety of military operational requirements and environments (contexts of use), as well as, the potential targeted attacks on the vulnerabilities of an AI algorithm may affect the reliability of the system.

To tackle the aforementioned issues, FaRADAI proposes to:

- Research and develop frugal AI methods for minimising data total size used for training and adaptation of AI systems, by developing automated data annotation techniques and allow rapid annotation of the collected data within EU. The AI methods will be enriched with domain adaptation techniques, aiming at improving the performance of AI models with a very limited amount of data, while minimizing the operator's need to intervene in cases of reusing the models under different conditions. Transfer and reinforcement learning techniques, will extend the knowledge of already existing models and provide environmental adaptation, targeting an AI framework tailored to the requirements of the military scenarios.
- Develop robust and explainable models that will boost the operator's perception and usage of the system's capabilities. A variety of methods will be developed which include but are not limited to:
    1. Hybrid AI techniques by combining different basic and DL-based methods, discriminative, generative, and evolutionary learning.
    2. Methods for improving robustness against adversarial attacks. Enabling logic-based representations of reasonable model behaviors, defined and expected by the human operators.
    3. Explainability metrics and mechanisms for the analysis and explanation of the decisions made by the AI models
- Fuse multimodal data, acquired by heterogeneous sources, in order to extract additional knowledge and provide a framework for enhanced planning and operational capabilities. Generative Learning tools will also be developed to account for enhanced threat assessment capabilities during mission definition and planning, incorporating cognitive analysis to provide quantitative and qualitative assessments of the potential threats. Lastly, AI-powered decision-making tools will be designed, developed and evaluated aiming to support mission planning and C2 in order to deliver an improved framework of situation awareness and intelligence.

The objective of FaRADAI is to contribute to the trustworthy implementation of AI models in defence applications, through research and development of new technologies that are designed to address the needs of a military operational environment.

Acknowledgements

This project has received funding from the European Defence Fund programme under grant agreement No 101103386. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Un-ion or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

1. Van Wynsberghe, A. (2021). Sustainable AI: AI for sustainability and the sustainability of AI. AI and Ethics, 1 (3), 213-218.
2. Furman, J., & Seamans, R. (2019). AI and the Economy. Innovation policy and the economy, 19 (1), 161-191.
3. Taylor, T. (2019). Artificial Intelligence in Defence: When AI Meets Defence Acquisition Processes and Behaviours. The RUSI Journal, 164 (5-6), 72-81.

FIBERMARS:

FIBER optic technology for Maritime Awareness and ReSilience

Dimitris Diagourtas[1], Andreas Papadimitriou[1], Charalampos Papadakos[1], Marios Moutzouris[1], Andronikos Balaskas[1], Bernd Drapp[2], Thomas Hamm[2], Daria Damm[2], Matthias Mildner[2], Paulo Chaves[3], Armando Fernandes[3], Max Goerler[4], Ivor Nissen[4], Finn Reikowski[4], Vassilis Karastathis[5], George Drakatos[5], Dimitris Venizelos[5], Aggelos Mouzakiotis[5], Konstantinos Papagiannakis[6], Victor Lobo[7], Hugo Policarpo[7]

[1] **SATWAYS Ltd,** Greece,

[2] **AP Sensing GMBH,** Germany,

[3] **INOV Instituto De Engenharia De Sistemas E Computadores Inovacao,** Portugal,

[4] **Wehrtechnische Dienstelle Für Schiffe Marinewaffen, Maritime Tecnologie Und Forschung,** Germany,

[5] **National Observatory of Athens, Greece**

[6] **Hellenic Navy,** Greece,

[7] **Centro de Investigação Naval (CINAV),** Portugal

Keywords

Distributed Acoustic Sensing (DAS), Fiber Optic Cable (FOC)

Extended Abstract

1.1 Introduction

The project "FIBER optic technology for Maritime Awareness and ReSilience" (FIBERMARS) is focusing on and advance the Distributed Acoustic Sensing (DAS) technology. DAS exploits the laser - induced Rayleigh backscattering in the Fiber Optic Cable (FOC) to detect incident acoustic waves. Feasibility studies are performed in an isolated-controlled environment for underwater testing as well as in real operational environments, also for extended testing periods. The expected impact includes the improvement of Maritime Situational Awareness with respect to existing technologies, along with the reduction of the acquisition and maintenance costs.

1.2 Problem statement

Currently, acoustic monitoring in coastal Critical Infrastructures (CI), in choke points and in open sea is performed either by arrays of hydrophones (fixed or towed), or by sonobuoys that are dropped/ejected from aircraft or ships conducting anti-sub marine warfare or underwater acoustic research. Both solutions are expensive and there is always the risk of losing the sensors in the field. Such acoustic technologies/sensors, which often deteriorate or get damaged due to the adverse conditions prevailing in the underwater environment, provide reliable information but with a limited range and high (per sensor) purchase and maintenance costs.

1.3 FIBERMARS Concept

FIBERMARS aims to enhance Maritime (underwater) Surveillance and Maritime Situational Awareness (MSA), via a very promising and low-cost (per sensor) technology, called Distributed Acoustic Sensing (DAS), that can turn FOCs to arrays of thousands of "virtual microphones". It is known that vessels can be detected by DAS technology. FIBERMARS is trying to develop detection, identification, classification and tracking algorithms for vessels and maybe submarines, in an effort to estimate the value of DAS technology for maritime surveillance.

The main advantage of DAS technology is that it can exploit either existing FOC infrastructure (telecom/power) at the sea floor, or new FOCs that can be installed in specific areas of interest.

The FIBERMARS solution's design is based on three core elements:

1. The FOC serves as the primary sensing element.
2. The DAS Interrogator is measuring the reflected acoustic waves.
3. The Data Collection Platform is gathering the output of the Ground Truth sensors.

Several feasibility studies are performed in three test sites (Portugal, Germany and Greece) that is including:

- Initial tests in controlled environments in Portugal and Germany
- Tests with new FOC deployment in all three sites
- Real operational environment testing by using existing telecom FOC in Greece and Portugal

The Feasibility Studies are based on acquiring data both from the FOC, through the DAS Interrogator and from the Data Collection Platform, gathering the output of traditional means of maritime surveillance such as hydrophones, radars, AIS receivers and E/O sensors, in order to cross corelate and verify the results.

Acknowledgements

This project has received funding from the European Union's "EDF-2021-OPEN-R: Open call focused on SMEs for research on innovative and future-oriented defence solutions" under grant agreement No. 101110375. This article reflects only the authors' views and the Directorate-General for Defence Industry and Space and the European Commission are not responsible for any use that may be made of the information it contains.

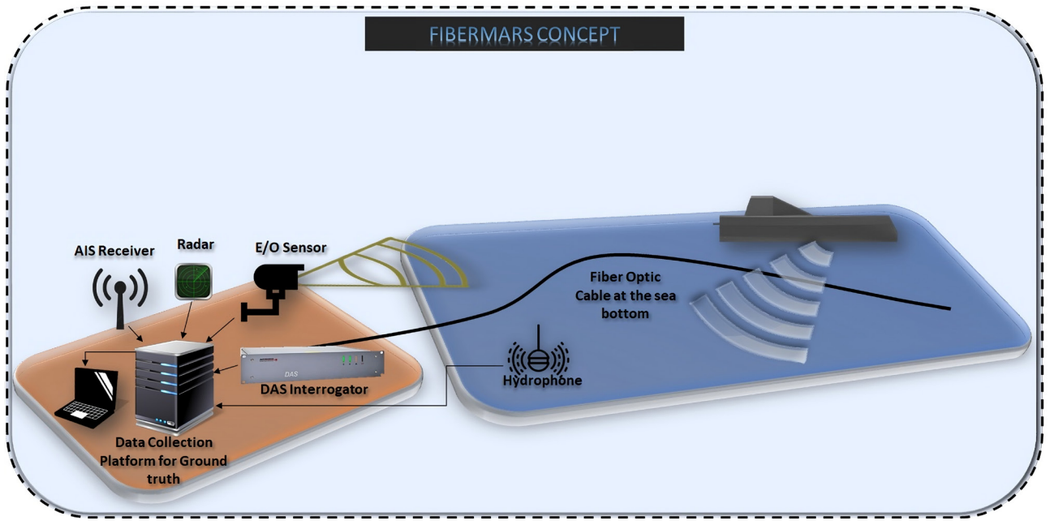


Figure 1: FIBERMARS Feasibility Studies Concept

TICHE:

Threats Identification by Collaborative vehicles for Human lifesaving against Explosives - TICHE

Pantelis Michalis, Nikos Frangakis, Makis Pachos, Theofilos Dimitriadis

iKnowHow S.A., Greece

Keywords

Hidden Threat Detection, Unmanned Vehicles, Sensors

Extended Abstract

The past armed conflicts around the globe, as for instance in Afghanistan, Iraq or Syria, have seen a dramatic rise in the use of Improvised Explosive Devices (IEDs) and landmines by adversaries. In operations taking place in those countries, 50% of soldier deaths in action are directly related to IEDs.

Furthermore, the Ukraine war and its linked increasing geopolitical tensions are driving high investments in the defence sector, contributing to the growth of artificial intelligence in defence market. A significant portion of the investment is dedicated to the procurement of AI in defence research.

The TICHE project aims to develop a novel multiplatform collaborative solution to detect and characterise IEDs and landmines in complex environments, using a combination of advanced sensors, information fusion from these sensors, and unmanned ground and aerial systems to extend the detection capabilities.

The developed solution will integrate both proven and experimental sensors, aiming to improve the state-of-the-art in hidden threats detection but also in terms of power consumption, transportability, communication, interfacing capability and continuous operation.

In the called scenario, collaborative UGV, mid size UAV and a swarm of hand size UAVs have the potential to be the most effective multiplatform solution for speed of intervention, automation, surveying, detection, sampling, identification and mapping the suspected area and therefore for retrieving critical information in support of military operations and lifesaving.

Figure 1

Acknowledgements

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

WEMOR:

WEMOR project: Wearable device for monitoring warfighter health and sustainability

Alexios Pagkozidis[1], Charalampos Papadakos[1], Leonidas Perlepe[1], Eleftherios Voumvourakis[1], Diagourtas Dimitrios[1], Antonis Kostaridis[1], Evangelos Sakkalis[2], Emmanouil Spanakis[2], Matthew Pediaditis[2], Kostas Ramantas[3], Héctor Mora[4], Alicia Mora[4], Nikolai Stoianov[5], Yantsislav Yanakiev[5], Carl Montan[6]

[1] **Satways Ltd,** Greece,

[2] **TRAQBEAT TECHNOLOGIES,**

[3] **Iquadrat,** Spain

[4] **OASI 233 SL,** Spain,

[5] **INSTITUT PO OTBRANA - BDI DEFENCE INSTITUTE,** Bulgaria,

[6] **Incisio AB,** Sweden

Keywords

Wearables, Military, Health Monitoring

Extended Abstract

There is strong awareness in Defence domain on effects of demanding military operations and settings on well-being, performance, and survivability of the soldiers. Unfortunately, while there is significant progress in mitigating issues, the current countermeasures to keep military personnel healthy are not always effective.

The WEMOR project studies the feasibility of a holistic health and wellness management system through a single wearable biomarker monitor device to maximise soldier effectiveness, readiness, protection and recovery. The envisioned system will enhance the performance and effectiveness of the individuals in military operations and increase the reliability of real-time health monitoring to optimize soldier protection.

Limitations of current wearable health monitoring applications in defence demonstrate the need for a) design the appropriate single device for physiological monitoring of military without sacrificing accuracy and comfort of the military operatives b) design and study novel analytics methods for soldier performance and conditions assessment and c) design appropriate decision support framework which will utilize the wearables data.

The project research is aiming to remove the significant bottlenecks that are preventing the transition of health monitoring through wearable devices in the defence domain. Till now defence wearable health monitoring was relied on using a) commercial grade wearable solutions b) dependency on data provided from multiple devices that result proprietary data and c) absence of appropriate decision support framework and systems.

To foster the successful study of health monitoring of wearable systems in scalable practice across Europe, the WEMOR project will develop the appropriate design and will study the applicability of the design across two countries (Spain and Bulgaria) to ensure good differentiation in the weather conditions, social and cultural environments.

Acknowledgements

This project has received funding from the European Defence Fund 2022 Programme (EDF-2022-LS-RA-SMERO) under Grant Agreement No. 101121488.

Image Credits

1. **pages 12-13:** Image by Vilius Kukanauskas from Pixabay
2. **pages 56-57:** Image by Pexels on Pixabay
3. **pages 72-73:** Image by freepik on Freepik
4. **pages 84-85:** Image by fanjianhua on Freepik
5. **pages 96-97:** Image by Markus Spiske on Unsplash
6. **pages 106-107:** Image by rawpixel.com on Freepik
7. **pages 114-115:** Image by ThisIsEngineering on Pexels
8. **pages 124-125:** Image by freepik on Freepik
9. **pages 130-131:** Image by freepik on Freepik
10. **pages 6, 148, cover & back cover:** Image by starline on Freepik

RISE SD 2024

Research and Innovation Symposium
for European Security 2024

Proceedings Book | Online edition