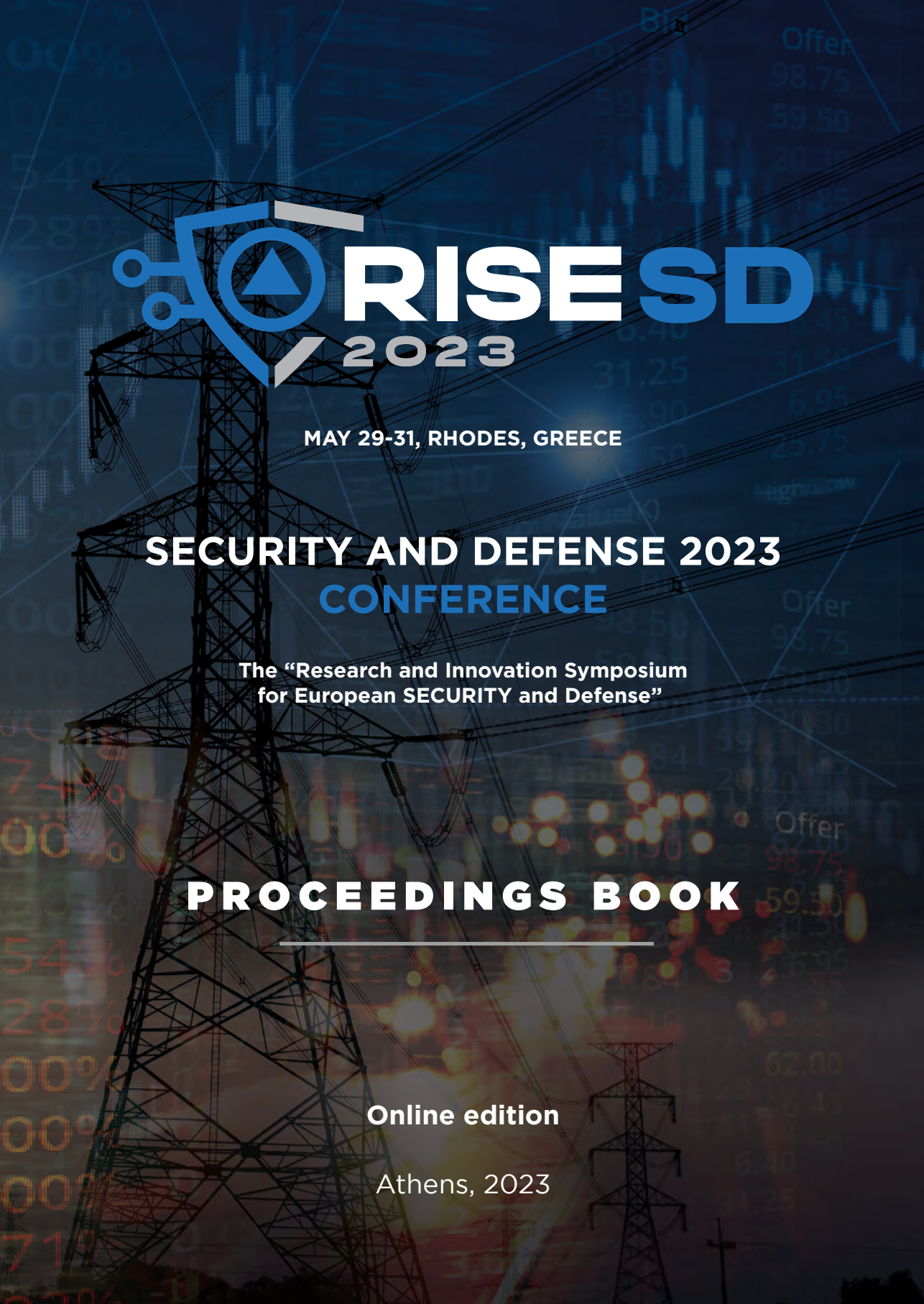


MAY 29-31, RHODES, GREECE

SECURITY AND DEFENSE 2023
CONFERENCE

The "Research and Innovation Symposium for European SECURITY and Defense"

PROCEEDINGS BOOK

Online edition

Athens, 2023

SECURITY AND DEFENSE 2023
CONFERENCE

MAY 29-31, RHODES, GREECE

PROCEEDINGS BOOK

Ilias Gkotsis[1], Nikolai Stoianov[2] and Dimitris Kavallieros[3]
Editors

1. Satways Ltd.
2. Bulgarian Defence Institute
3. Information Technologies Institute - Centre for Research and Technology Hellas

Online edition

Athens, 2023

Imprint
2023 Satways Ltd.

Published by:
Satways Ltd.
Information Technologies Institute - Centre for Research and Technology Hellas
Bulgarian Defence Institute

Proceedings of the Research and Innovation Symposium for European SECURITY and Defense – RISE-SD Conference, May 29-31, 2023

1st edition, 2023 | Satways Ltd., Athens
ISSN: 2945-1183

Layout and Technical editing: *Katerina Valouma*

Suggested citation:
Cover picture: Author/s, "Title of paper", in Proceedings of RISE-SD2023 "Research and Innovation Symposium for European SECURITY and Defence", Rhodes (Greece, 2023), pp. page numbers.

The papers appearing in this book compose the proceedings of the RISE-SD2023 event and the relevant "Research and Innovation Symposium for European SECURITY and Defence" cited on this volume's cover and title page. Papers were selected by the Organising Committee to be presented in an oral format and were subject to review by the program committee.

FOREWORD

We are pleased to introduce this collection of proceedings linked to the presentations made in the context of the Research and Innovation Symposium for European SECURITY and Defense 2023 (RISE-SD2023).

This conference brought together experts from across the crisis management, physical and cyber security, critical infrastructure protection, border management and defense technology spectrum to present, discuss and showcase research results and some of the most innovative solutions developed in the context of relevant European R&D projects.

The papers and presentations in these proceedings examine several aspects of security and defense challenges our world faces nowadays and offer insights into the related groundbreaking technologies and strategies being developed to address these challenges.

From cyber threats to natural disasters, this collection offers a panorama of the E.U. research and innovation potential, being a valuable resource for anyone seeking to understand the latest developments and best practices in crisis management and defense technology.

We would like to thank all the contributors to this collection for their hard work and dedication to advancing E.U. security research and innovation, and we look forward to seeing the impact of their efforts on the world at large.

The RISE-SD2023 Organizing Committee

TABLE OF CONTENTS

01

CIVIL PROTECTION AND DISASTER-RESILIENT SOCIETIES

aqua3S

aqua3S

Integration of innovative technologies for safety and security in drinking water networks and the paradigm of aqua3S

A. Moumtzidou[1], S. Kintzios[1], A. Karakostas[2], L. Vamvakeridou-Lyroudia[3], K. Valta[3], E. Ouzounoglou[4], A. Chen[2], H. Gibson[5], D. Cabús[6], E. Piccoli[7], P. Cousin[8], M. Mirachtsi[9], T. Jacquemard[10], F. Lombardo[11], A. Christodoulou[12], S. Deveughele[13], S. Charalambous[14], E. Chauveheid[15], M. Aleksova[16], E. Rumenova[17], S. Vrochidis[1], I. Kompatsiaris[1]

1. ITI - CERTH
2. DRAXIS
3. UNEXE
4. ICCS
5. CENTRIC
6. EVERIS SPAIN
7. ACEGAS-APS
8. EGLOBALMARK
9. WaterEurope
10. TRI
11. AAWA
12. EYATH
13. 3S
14. WBL
15. VIVAQUA
16. SOFYISKA
17. ViK

Abstract

aqua3S[1] is a project funded by the European Union's Horizon 2020 Research and Innovation Program under the topic "Pre-normative research and demonstration for disaster-resilient societies". aqua3S started in September 2019 and finished on December 2022 and it involved 23 partners across Europe. In this context, we unfold the concept and approach, its use cases of application, and the impact it aims to achieve.

1. https://aqua3s.eu/

Introduction

Access to high-quality drinking water is crucial for promoting individual health and well-being. Drinking water networks are considered critical infrastructure, and their safety and security must be protected to prevent large-scale disasters for communities. Despite several proposed technologies for analyzing drinking water, integrating them into existing safety networks is a challenge. The aqua3S project proposes standardization methods and strategies to ensure water safety and security by offering an efficient detection system that combines data from various sources to close the divide of the real utility providers needs and innovative technology solutions. This system aids professionals from the water and medical sectors, first responders, and utility providers in handling water-related crises.

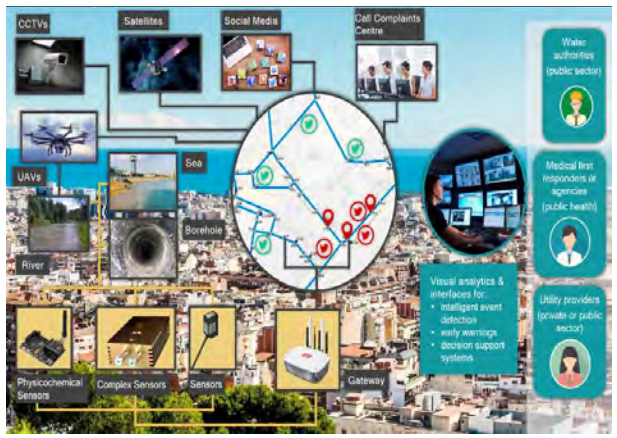


Figure 1 *depicts the concept of aqua3S and its stakeholders. Relevant projects to aqua3S, which the consortium built upon, are the following: H2020 beAWARE [2], H2020 CUTLER [3], FP7 ICeWater [4], H2020 SEC ROBORDER [5], H2020 CALLISTO [6], and FP7-ENV-2012 Wesenseit [7].*

Approach

aqua3S is a platform that integrates technologies from various fields, including sensors, IoT, satellite data analysis, decision support systems, and crisis management to address water sector issues. The platform's main objectives are to propose innovative sensor technologies, develop strategies and methods for water facilities to integrate solutions for water safety, create early warning systems, estimate infrastructure resilience, and model crisis events. aqua3S equips water distribution networks with innovative sensors and uses data from various sources, such as UAVs, CCTV cameras, satellite imagery, and citizen reports. The platform also aims to raise awareness through bottom-up approaches, engage first responders, and provide

scalable solutions through optimized algorithms. The platform was developed based on user needs and gaps in legacy systems and takes security requirements into consideration to help protect water networks from hazardous circumstances.

Technologies

aqua3S aims to establish standardized methods and strategies for water safety and security. To ensure its goals aqua3S develops and integrates innovative technologies and legacy systems such as a high-precision key point spectroscopic sensors capable of detecting aqueous ammonia, and refractive index sensors detecting changes in water composition. Sensors deployed at key points throughout the water distribution network and along with the measurements collected by COTS sensors provide an early warning sign. More data obtained from other types of sensors, including Unmanned Aerial Vehicles (UAVs), CCTV cameras, satellites, and citizen observations enhancing the process. In example, detect or locate harmful: substances and flood risks using satellite imagery; major distribution issues using citizens' feedback from social media and call centers; potential offenders near water resources using UAV and CCTV images. Moreover, aqua3S enhances the retrieved information by semantically enriching it and considering existing knowledge. Smart data connection allows for alarms to be generated when anomalies are detected in the water network, and to evaluate the severity of crises related to floods or water quality, and interventions using real-time sensor data for stakeholder decision-making. This information is visualized through bespoke visual analytics tools, including a 3D representation map and graphs, on a shared platform. Additionally, a guide is available to assess systems' vulnerability and preparedness for crises. Finally, aqua3S produces standardized warning messages during a crisis, disseminated through the platform to raise awareness and encourage knowledge sharing.
All the developed technologies within aqua3S are compatible with FIWARE[2] to fully utilize platform's benefits. Although a platform was developed to host all the aforementioned technologies

Applications

Most of the main challenges faced in all seven Pilot Use Cases (PUC) of aqua3S, along with their characteristics are following. The project used an updated TRIAL Guidance[3] methodology from DRIVER+ project to test and validate the technologies developed within aqua3S in both routine and crisis scenarios. Detailed questionnaires assessed user satisfaction with the usability, execution of exercises, and usefulness of the aqua3S platform and individual modules.
PUC1- Monitoring the safety and security of the Trieste Aqueduct: PUC1 is responsible for ensuring the safety and security of the Trieste Aqueduct, which is the primary source of drinking water for Trieste. The aqueduct draws water from flood-prone wells, emphasizing the need for continuous monitoring. Transboundary rivers in the area are monitored using connected sensors to detect anomalies and generate timely alerts. Satellite imagery is also utilized to assess flood severity and aid in disaster recovery planning.
PUC2 - Aliakmonas river and Thessaloniki Water Treatment Plant monitoring: The core responsibility of PUC2 is to oversee the Polyfytos artificial lake and the river channel that supplies surface water to the Thessaloniki Water Treatment Plant. PUC2 aims to mitigate various water safety risks by sensors deployment at key river locations,and utilizing satellite data, UAVs, and CCTVs for close lake monitoring. Early detection and warning of harmful events are prioritized.
PUC3 - Monitoring safety and security of the Sénéo Water Supply System: PUC3 is responsible for ensuring the safety and security of the water supply system in the western part of Paris. To achieve this, the aqua3S project addresses several key areas, including forecasting water demand, monitoring water quality, detecting abnormal water quality events automatically, and detecting leaks at an early stage.
PUC4 - Desalinated and treated surface water monitoring in Lemesos: The main goal of PUC4 is to monitor the quality of desalinated and treated surface water in Lemesos. Existing sensors provide continuous updates on water level, flow, and pressure, but fluctuations can affect water quality. PUC4 monitors data from the dam, satellites, and call complaints, issuing early warnings and alerts in case of anomalies for a more comprehensive understanding.
PUC5 - Monitoring the water supply system in the city of Brussels: PUC5 monitors the drinking water distribution network in Brussels, serving over 1 million people. To provide continuous monitoring, multiple sensors are installed and data from citizens is utilized, enabling timely alarms in case of incidents.
PUC6 - Monitoring of Iskar dam and drinking water network in Sofia: PUC6 aims to monitor untreated water quality in the Iskar dam and drinking water supply in Sofia with online sensors detecting contamination and providing alerts. Satellite, drone

2. https://www.fiware.org
3. https://www.driver-project.eu/trial-guidance-methodology/

observations, quality parameter monitoring, and ultrasonic surveillance of algae are used.

PUC7 - Monitoring of the water quality parameters in Botevgrad: PUC7 monitors Botevgrad's treatment plant and water supply network. However, there is no current way to detect deviations (microbiological or physicochemical) from expected water quality. To solve this, aqua3S added sensors for continuous monitoring and alerts.

Impact

aqua3S aims to have significant impacts on society, science, and the economy. Societally, it enhances water authorities' ability to identify and solve problems through collaboration and information sharing. Scientifically, it develops innovative detection technology for substances in water, natural hazards via satellite data, social awareness through monitoring social media, threat detection in water distribution networks, crisis management models, and crisis severity classification. Economically, it improves substance detection efficiency, reduces monitoring solution costs, promotes platform reusability, and lowers water network surveillance costs.

References

1. aqua3S project, https://cordis.europa.eu/project/id/832876
2. beAWARE project, https://cordis.europa.eu/project/id/700475
3. CUTLER project, https://cordis.europa.eu/project/id/770469
4. ICeWater project, https://cordis.europa.eu/project/id/317624
5. ROBORDER project, https://cordis.europa.eu/project/id/740593
6. Wesenseit project, https://cordis.europa.eu/project/id/308429

Co-Protect

Co-Protect: Greek cluster for cooperative and interoperable Crisis and Disaster management solutions

George Eftychidis[1], Ilias Gkotsis[1] and Dimitris Diagourtas[1]

1. Satways Ltd

Strengthening the use of civil protection solutions through interoperability

Co-Protect is a cluster project supported by the Greek General Secretariat of Research and Innovation, which coordinates the effort of several technological enterprises and SMEs in Greece aiming to deliver innovation by bringing together and upgrading high TRL products, systems, and services related to the management and response to natural disasters, environmental crises, and civil protection emergencies. Co-Protect is a pioneering initiative of the Greek community of SMEs, active in environmental protection and security solutions, to deliver interoperable products that may have a global market perspective. The project is part of the Greek Disaster Resilience Innovation Cluster, Defkalion (DRIC), which is a partnership focused on protecting the environment and preventing risks to public safety.

The members of the consortium are small to medium-sized enterprises (SMEs) that are already involved in businesses related to crisis and disaster management in Greece and other international markets. Leading research institutions in Greece are also collaborating with the consortium to provide advanced technology components and modules with a high Technology Readiness Level (TRL). These components can be integrated into Co-Protect 's commercial solutions. By working together, the consortium can address any operational gaps and technological limitations of existing products, resulting in competitive solutions that can be offered to a wide market.

Co-Protect offers interoperable solutions that can assist various public and private organizations. These include Civil Protection Organizations, Emergency Manage-

ment Services, Environmental organizations, Defence Authorities, Critical Infrastructure managers and operators, Regional and Local Authorities, and Law enforcement agencies like Fire Brigades and Police Departments. These solutions can aid in executing operational tasks and missions effectively.

Co-Protect 's strategy is to establish valuable local and international partnerships, enhance cooperation amongst Greek SMEs, and introduce well-established safety and security products to European and global markets.

The project aims to provide components that can work together seamlessly and be easily integrated into a common information management platform to assist with disaster and crisis management. The anticipated result is improved disaster and crisis management support. Co-Protect's outcome includes:

- an interoperability framework at the level of data models and services to standardize the communication and sharing between current products, services, methods, and solutions of the platform of Co-Protect components as well as for others that will be developed in the future.
- technological solutions that provide early warning for earthquakes and rapid damage assessment based on risk assessment reasoning, fragility curves, and networks of specialized sensors and digital equipment.
– data modeling solutions for flood events and extreme weather forecasting, which can help with preparedness and decision-making.
– solutions for managing wildfires, which include mapping risks, detecting and locating fire spots, simulating the spread of fires, and providing support for fire operations.
- solutions that help with the surveillance and monitoring of security issues in critical infrastructures.

The Co-Protect product repository offers various tools and solutions to assist with disaster and crisis management tasks. The repository is organized according to the risk category (extreme weather, floods, wildfires, earthquakes, and protection of critical entities), and the relevant components are compatible with platforms that allow for interoperable data and services.

The solutions should share common information and properly model the data exchange to provide interoperable services. This can be achieved through the Common Interoperability Framework (CIF) of Co-Protect, which all systems and applications integrated into the project's platforms must follow. The CIF comprises of two models - data and service models - that allow maximum cooperation and exchange between the dispersed and different applications that can fit onto the platform.

At Co-Protect, we aim to expand our reach worldwide by working alongside EU entities and the European Security Industry. We strive to improve the capabilities of Greek small and medium-sized enterprises by promoting cooperation and highlighting the benefits of interoperability in technology, organization, and business.

Acknowledgements

This project, coded as ΓΓ2CL-0363842, has received funding from the Greek General Secretariat for Research and Innovation (GGEK) according to Decision 75101 - 25-07-2022 (ΑΔΑ: 65Κ346ΜΤΛΡ-0ΡΘ). This article reflects only the authors' views, and the Greek General Secretariat for Research and Innovation is not responsible for any use that may be made of the information it contains.

FIREURISK

FirEUrisk: Dissecting risk to prevent extreme wildfires

Ioannis Gitas[1], George Eftychidis[1], Domingos Viegas[2], Emilio Chuvieco[3]

1. Laboratory of Forest Management and Remote Sensing, School of Forestry and Natural Environment, Aristotle University of Thessaloniki
2. Department of Mechanical Engineering, CEIF/ADAI, University of Coimbra
3. Universidad de Alcalá, Environmental Remote Sensing Research Group, Department of Geology, Geography and the Environment

The FirEUrisk research contribution to the E.U. wildfire management capacity

Wildfires are a serious threat to human activities, assets, and infrastructure. The FirEUrisk project aims to analyze risk factors associated with wildfires and develop effective strategies to manage and minimize their impact. The project also consid-ers the impact of climate change on wildfires in the EU and explores adaptation approaches to mitigate future risks. FirEUrisk has created a comprehensive strategy for man-aging wildfires, which includes risk assessment, risk reduction, and planning for future adaptation (as shown on the left in Fig. 1). The project's research will be tested at various levels, from local to EU-wide scales, and will benefit a wide range of users, including managers, decision-makers, and policymakers at European, na-tional, and regional levels. The strategy will cover a range of spatial and temporal scales. To test the effectiveness of the research, FirEUrisk will use five pilot sites in Greece, Spain, Portugal, Ger-many, and Sweden, as well as various demonstration areas (as shown on the right in Fig. 1).

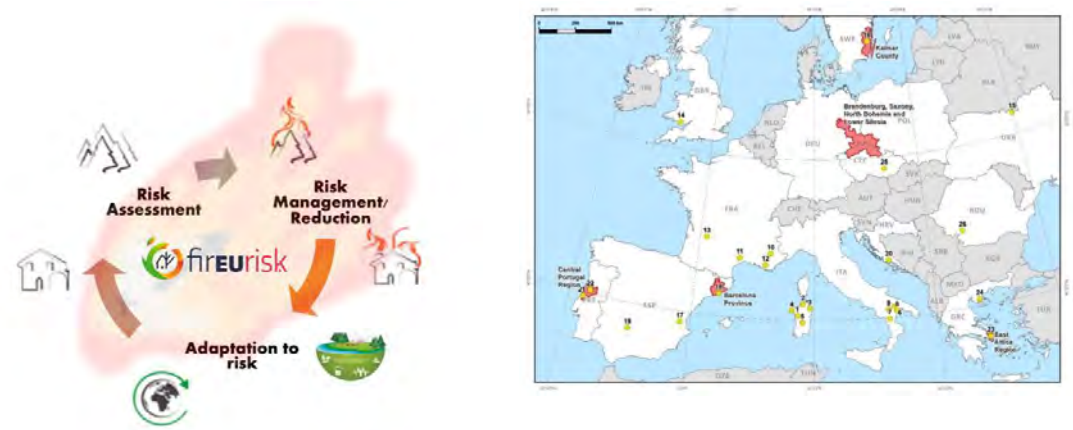


Figure 1. *FirEUrisk wildfire management approach (left) and Network of Pilot sites and demonstration areas (right)*

The goal of FirEUrisk is to provide scientific products, tools, and evidence to support a comprehensive approach to wildfire management. The project analyzes wildfire risk as both a challenge and an oppor-tunity to landscape fire management issues. The assessment considers factors such as danger, vulnerabil-ity, and exposure, and scientifically proven methods are used to evaluate and manage the risk. The project identifies areas where risk reduction is necessary and maps out appropriate strate-gies for managing the risk. FirEUrisk has three work modules - assessment, reduc-tion/management, and adaptation - that are linked together to create an integrated and holistic wildfire management proposal (Fig.2). The project creates procedures to modify factors that control the assessed level of risk in the short and mid-term (mitigation) and long-term (adaptation).
Beyond the current scientific work on wildfire danger rating, FirEUrisk aims to iden-tify the factors that potentially influence the impact of fire on society, the environ-ment, and the economy and elaborate ways for reducing their relevant impact. The research also anticipates how these factors may change in the 2 medium and long term, due to climate and socio-economic changes and develop strategies to miti-gate the relative risk.

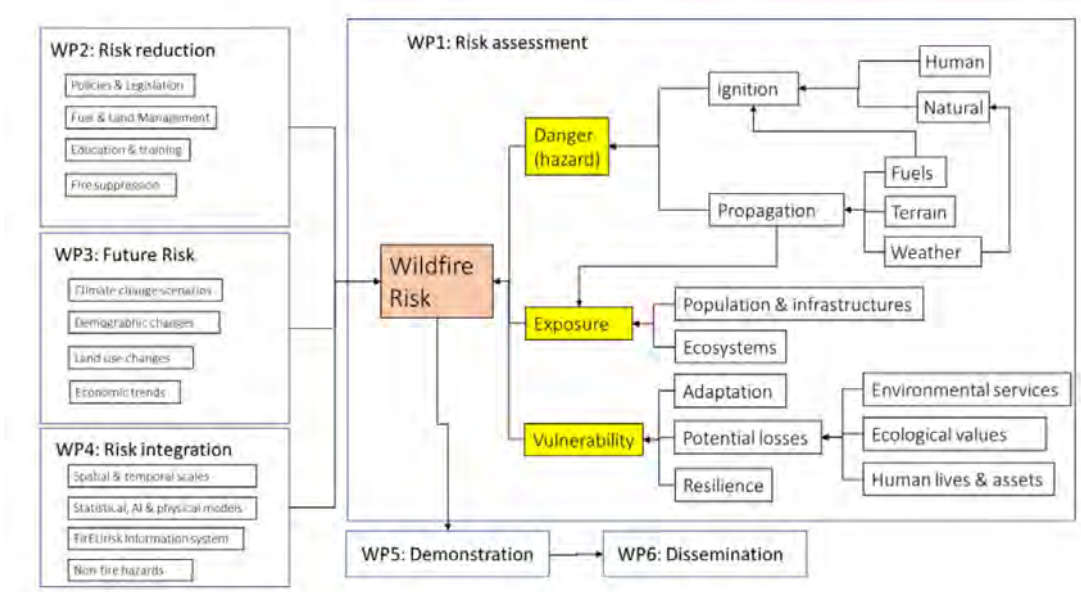


Figure 2. *The Fireurisk conceptual approach for risk-driven wildfire management*

The FirEUrisk research activity focuses on extreme or high-impact fires and fires in wildland-urban in-terface areas. It examines forest and fuel management strategies as well as land management strategies to identify and prove their ability to reduce risk. The research also considers the potential impact of policies and legislation, such as land use change, human activity monitoring, and fire ignitions, on defining the level of fire risk and the resilience of EU landscapes.

FirEUrisk offers a range of products to aid in the comprehensive management of wildfires. These include maps at varying scales, software modules, methodologies, and policy recommendations. At the midpoint of the project, FirEUrisk has already accomplished a lot, such as creating a methodology for identifying forest fuel types and producing a Fuel Map of the European Territory (seen on the left in Fig.3). Ad-di-tionally, the Consortium has generated Pan-European maps that evaluate ecolog-ical vulnerability, human fire ignitions, the importance of risk factors, and suitability of Land Management Strategies (seen on the right in Fig.3). A mobile application that allows citizens to participate in wildfire research is also devel-oped.

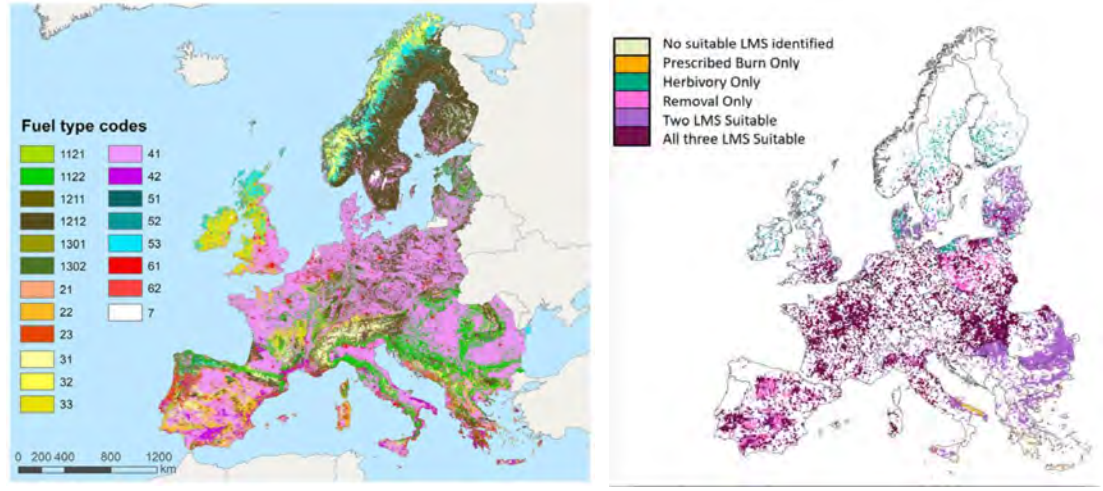


Figure 3. *FirEUrisk Fuel Type classification (right) and Land Management Strategies suit-ability for fuel management (left) European maps (Aragoneses et al. 2023)*

FirEUrisk aims to create a conceptual framework that integrates various phases of risk management into a joint plan. This approach will move us away from the unproductive conflict between wildfire prevention and suppression and towards a more inclusive strategy. The project's product line will be made more 3 accessible to potential users with the implementation of an information system that allows for easy explo-ration and familiarization.

Acknowledgements

The FirEUrisk project has been granted funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 101003890. 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. Aragoneses E., García M., Salis M., Ribeiro L.M., and Chuvieco E., 2023, Classifica-tion and mapping of European fuels using a hierarchical, multipurpose fuel classi-fication system, Earth System Science Data, Vol. 15, Issue 3, 1287–1315, DOI: https://doi.org/10.5194/essd-15-1287-2023

2. Chuvieco. E., Yebra M., Martino S., Thonicke K., Gomez-Gimenez M., San-Miguel-Ayanz J., Oom D., Velea R., Mouillot F., Molina J.R., Miranda A., Lopes D., Salis M., Bugarić M., Sofiev M., Kadantsev E., Gitas I.Z., Stavrakoudis D., Eftychidis G., Bar-Massada A., Neidermeier A., Pampanoni V., Pettinari L.M., Arrogante-Funes F., Ochoa C., Moreira B., Viegas D.X.,. Towards an integrated approach to wild-fire risk assessment: when, where, what and how may the landscapes burn and with what consequences? (submitted for review)

iProcureNet

Is public procurement hindering factor in the uptake of Innovation? - iProcureNet

Jozef Kubinec[1]

1. I.C.T. Procurement Department, Ministry of Interior of the Slovak Republic.

1. Is public procurement hindering factor in the uptake of Innovation?

End-users in the security sector often perceive public procurement as hindering innovation uptake. iProcureNet conducted an internal survey among the consortium on the main obstacles to innovation uptake. Several answers indicated that end users observe procurement as an obstacle to obtaining innovative solutions for their needs.

The presentation and, eventually, the paper will debate the role of public procurement in security research and Innovation, present the steps that the project iProcureNet is taking to promote Innovation, and ultimately answer the question if public procurement is a hindering factor in innovation uptake.

1.1 iProcureNet at the Heart of security innovation

To battle with this opinion that public procurement is hindering factor of innovation uptake, the iProcureNet project envisaged creating an ecosystem of procurers, prescribers, legal advisors and other key stakeholders of security procurement to share and analyse procurement trends and needs, develop common and standardised practices from the technical, legal and financial perspectives, and open pathways for joint cross border public procurement.

Furthermore, iProcureNet dedicated its activities to promoting Innovation in security procurement and supporting European procurers in cross-border joint procurement and innovation procurement. These actions should convince policymakers and end-users that it is essential to turn the narrative into a more innovative

procurement in the security sector, ultimately promoting the idea that procurement can catalyse Innovation.

1.2 Procurement Instruments to promote Innovation

There are already well-established mechanisms to promote Innovation in the case of solutions that are not yet on the market or not commercially available. These are pre-commercial procurement and innovation procurement. Expect these mechanisms; the papers will identify other public procurement instruments that can promote Innovation even in the case of procurement of COTS, such as preliminary market consultation, value engineering and functional specifications.

1.3 Joint cross-border public procurement

Joint cross-border public procurement (JCBPP) is an innovative way of procurement. A promising mechanism of efficient purchasing as well as a strategic tool for the positive use of purchasing power on the market, it enables sharing of costs, securing economics of scale and developing Innovation.1

1.4 Pre-commercial Procurement and Public Procurement of innovative solutions

PCP can be described as a specific approach to procuring R&D services that involve competitive development in phases, risk-benefit sharing under market conditions, and where there is a clear separation between the PCP. and the deployment of commercial volumes of end products (potential follow-up PPI).2 On the other hand, Public procurement of innovative solutions (PPI)' means procurement where contracting authorities act as a launch customer of creative goods or services which are not yet available on a large scale.3 PPI are part of public procurement tenders because they are done according to the rules of EU directives on public procurement.

1.5 Preliminary market consultation as a legal and flexible way to communicate with suppliers

One of the effective ways to promote Innovation and learn about new innovative solutions is to conduct open market consultation or, as stated in article 40 of the Directive 2014/24/EU, preliminary market consultation (PMC.). According to Voda and Jobse "specifically in case of innovation procurement, market consultation plays a crucial role due to the fact that the innovation cycle is normally longer than the procurement cycle". 4

PMC. can be described as a formalised dialogue between the contracting authority and other entities (economic operators, suppliers or independent experts), aiming to obtain answers to how the contracting authority's problems can be solved.
Prior market consultation is a cornerstone of innovation procurement, providing advance notice to the market of opportunities and the unmet needs of their customers, allowing both time and valuable insights to suppliers to direct their business plans. On the other side, buyers will understand the market's appetite, capacity and capability to meet their needs and the timeframes involved. Experience from prior market engagement and consultations conducted is that it is welcomed by suppliers who find the process and access to customers beneficial.

1.6 Functional Specification vs descriptive requirements

According to the E.C. notice – Guidance on Innovation Procurement, "with descriptive technical specifications, the public buyer prescribes the detailed solution and bears full responsibility for its quality and performance levels." 5
On the other hand, when it comes to functional specifications, "shift the responsibility for achieving better results to the market. The public buyer sets minimum requirements to avoid an abnormally low-performing tender but is not overly prescriptive regarding the means of achieving a desired outcome. Economic operators enjoy openness and flexibility to reach the optimal performance." 6
Functional specifications should be preferred over technical specifications because they focus on long-term needs. It was mentioned in the online survey conducted by iProcurenet as a suggestion of good practice when referring specifically to PCP. Still, it can also be applied to public procurement tenders if the contracting authority wants to promote Innovation. According to the EC Guidance Notice on Innovation Procurement, "functional requirements are far more innovation-friendly" 8. This approach of using functional specifications was followed by 80% of the five EC-funded innovation procurement projects in the security sector mentioned in the assessment report on the performance of EC-funded innovation procurement projects in the security sector.7

1.7 Promoting Innovation by value engineering

C.A.s should, when drafting the tender documents and the contractual clauses, consider using the value engineering clauses to promote Innovation. In the procurement of COTS, the use of value engineering would be, for example, advisable in contracts where maintenance is a significant part of the value of the contract. For instance,

in the case of tender for higher-value drones, the maintenance cost should be considered when evaluating supplier offers. Suppose the value engineering clauses are used in the tender for drones when the supplier presents how to make maintenance more practical and cheaper during the contract. In that case, the savings should be split between the contracting authority and the supplier.

1.8 Conclusion remarks

In the paper, we debated the role of public procurement in security research and presented several procurement instruments that can promote innovation uptake. The frustration of end-users complaining about public procurement as an obstacle to Innovation could be addressed by procurement departments by explaining these instruments. It is also vital to the success of innovation procurement that the end users are involved in these procurement instruments; for example, they should be part of the team responsible for conducting preliminary market consultation.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 832875. 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. B. Heuninckx. Aggregated Procurement under Directive 2014/24/E.U.: Lessons from the Defence Sector, (2018) 27 P.P.L.R., 189; G. M. Racca & C. R. Yukins, Introduction: The Promise and Perils of Innovation in G. M. Racca – C. R. Yukins, eds., Cross-Border Procurement, in Joint Public Procurement and Innovation: Lessons Across Borders. Bruylant, 2019, available - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3486897 (September 28, 2020), 14.
2. eafip Toolkit, Module 3, p. 7, available at http://eafip.eu/toolkit/module-3-2/
3. eafip Toolkit, Module 3, p. 7, available at http://eafip.eu/toolkit/module-3-2/
4. O.P. Voda, C. Jobse, Rules and Boundaries Surrounding Market Consultations in Innovation Procurement, European Procurement & Public Private Partnership Law Review , Vol. 11, No. 3 (2016), pp. 179-193
5. EC notice – Guidance on Innovation procurement, European Commision, C(2021) 4320 final, 2021 available at https://ec.europa.eu/docsroom/documents/45975
6. EC notice – Guidance on Innovation procurement, European Commision, C(2021) 4320 final, 2021 available at https://ec.europa.eu/docsroom/documents/45975
7. Assessment report on the performance of the EC funded Innovation Procurement projects in the security field according to the EC Guidance Notice on Innovation Procurement, available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/industry-for-security/assessment_report_innovation_procurement_dg_home_final.pdf

PathoCERT

Enhancing pathogen contamination incident management through advanced operational picture and collaboration among incident commanders and first responders

Katerina Valouma[1], Leonidas Perlepes[1], Lefteris Voumvourakis[1], Antonis Kostaridis[1], Iosif Vourvachis[2], Dimitris Iliadis[2]

1. Satways Ltd.
2. Hellenic Rescue Team

1. PathoCERT challenges and objectives

Pathogens are a determining factor in emergency response due to their life-threatening nature, both for the public as well as for the First Responder (FR) safety. Waterborne pathogen contamination events can occur anywhere, and may be caused by various reasons, i.e. natural events, accidents or malicious attacks, illegal activities and cascading effects. To manage such incidents, FRs have expressed the need for a number of new technologies and tools, including but not limited to, sensors for rapid detection of pathogen contaminations, technologies for safe water sampling, decision support tools, tools to isolate the contaminant source and to conduct forensic investigation, restoration guidelines, etc.

To ensure the design and deployment of better products, services and/or governance mechanisms with a higher likelihood of effectiveness, the project relies on participatory and co-creative approaches. PathoCERT's multi-stakeholder engagement approach builds upon several interlinked activities, among others the Engagement of stakeholders via the establishment of 6 Communities of Practice. To identify relevant actors and analyse their interconnections, relationships and interest within; and to form an understanding of the current situation or status quo of a system, PathoCERT follows the stakeholder mapping methodology and baseline requirement analysis.

The stakeholder mapping and baseline requirement analysis was conducted by local consortium partners of each region under study and which will host the validation tests and demonstration exercises. Within PathoCERT the baseline requirement analysis developed a good understanding of the current emergency response and disaster management systems in each target city or region, including applied technologies, and main challenges and opportunities of improvement within. The examination and analysis of requirements, needs, challenges and opportunities are central to ensure that the project develops and tests appropriate solutions that contribute to improving and advancing the emergency and disaster management system.

More specifically, the emergency and disaster management system in Greece, is already well advanced and keeps track of the most recent developments. Nonetheless, there are some opportunities for change and further improvement. The need of increased coordination among operational actors has been identified. In general, operational entities are effective in following and implementing the emergency civil protection plans throughout the various steps and phases. Nonetheless, factors such as scale or timing of disaster, reduced human resources, frequent staff changes, improper definition of each actor's role and responsibilities, as well as bureaucracy, can diminish this effectiveness. Accordingly, providing relevant guidelines and clarification to each actor involved, on their roles and responsibilities in emergency management would support in effectively addressing such a challenge. In this direction, PathoCERT project aims to strengthen the coordination capability of the FRs during such incidents, allowing the rapid and accurate detection of pathogens, improving their situational awareness, and improving their ability to control and mitigate emergency situations involving waterborne pathogens. Overall, the new solutions will address a different part of the FR organization chain, starting from the individual responder in the field, to the Command-and-Control Centre which coordinates the operations in the field, and the Coordination Center in the Headquarters that monitor and provide information to the Incident Management System. Thus, PathoCERT is equipped with an incident management system, the PathoIMS component, that is planned to enable the monitoring and coordination of the response activities executed by FRs.

2. PathoIMS: Incident Management System

PathoIMS is the application that provides incident management capabilities to the PathoCERT platform. It is planned to be used by the commanders in control rooms

and/or by the local commander on the field (near the real location of the incident). To this end, PathoIMS receives information about the active alerts that have been detected and reported by the PathoCERT platform. Through the PathoIMS, commanders are able to manage the related response activities that are required. Information exchange between the commanders at the headquarters and the incident commanders on the field will be enabled, as. PathoIMS is developed to be deployed in both headquarters (desktop application) and on mobile control centres or team leaders (mobile application), allowing the provision of a common operational picture.

In more details, the desktop version of the PathoIMS is provided to the commanders at the headquarters and supports an advanced set of incident management functionalities. On the other side, the functionalities and the graphical user interface of the mobile/tablet version is optimised to the small size of the screen of the devices and to the capabilities that are required by the commanders on the field/mobile centres. Both types of PathoIMS applications are synchronized, presenting a common picture of the situation to all users, adapted and enhanced based on their responsibilities and access rights.

The PathoIMS capabilities have been based, designed, developed, and verified against the requirements and feedback provided by the end-users during the several Communities of Practice (CoP) events organised within the project, and the overall framework architecture, user stories and technical specifications that have been discussed as part of the project activities.

PathoIMS capabilities offered, include but are not limited to, Incident Management, Alarm Management, Resource Tracking, Support of Standard Operational Procedures, Visual presentation of operational information (map, tabular views), Reporting, etc., all of which are demonstrated and validated during the pilots of the project and specifically in Cyprus, Greece, Bulgaria and Spain. Through the live demonstration and exercise-based pilots, the developed tools and technologies will be tested, validated and evaluated by internal and external stakeholders. Specifically, within the pilot in Thessaloniki (Greece) IMS capabilities will be tested as part of an exercise scenario related to water pathogen contamination due to extreme rainfall phenomena that cause flooding on the river Axios, in the western suburbs of Thessaloniki. The impact of the flood affects both Water Supply & Sewage Company and Hellenic Rescue Team, the main actors of this exercise, who will get a hands one experience of the capabilities offered and the impact of the tools with regards to the management of such an incident.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883484. 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.

Pyrolife

Proposed actions towards streamlining Europe wide prevention strategies in wildfire management

Pooja Pandey[1], George Boustras[1], Miriam Arenas Coneio[2], Núria Prat-Guitart[3], Guillermo Rein[4]

1. Centre of Excellence in Innovation and Technology - European University Cyprus
2. Estudis de Psicologia i Ciències de l'Educació – Universitat Oberta de Catalunya
3. Pau Costa Foundation
4. Imperial College London

Aim and Purpose

Fires are essential and a natural process that aid in shaping the landscape of Earth. This paper is aimed at identifying the best practices for preventing wildfires across the European Union. The goal here is not to promote complete wildfire exclusion, but to reduce the likelihood of fire ignition and manage the growth and intensity of extreme fire events.

This is accomplished by first identifying the operational factors that affect the wildfire management and then making suggestions for wildfire prevention based on those factors. Based on the interviews conducted, some of the actions have been proposed towards streamlining Cyprus wide prevention strategies, followed by a list of the wildfire prevention activities categorized under the operation prevention component of Education (considered as one of the key components in raising awareness about wildfires in Cyprus) to aid the audience.

Audience - The deliverable is particularly useful for those people and organizations involved directly and indirectly in planning, implementing, and improving wildfire prevention measures. This includes wildfire managers, policy-decision makers, and scientists. 2

Additionally, this deliverable can also be useful to the media to further tailor wildfire information on prevention strategies.

Conclusion - Wildfires are a significant and recurring threat in Cyprus, therefore shifting towards an integrated approach might be a helpful solution to reduce the likelihood of extreme wildfire event. This approach could involve various initiatives such as doing more adult education, high visibility patrolling, enforcing laws, or training in preventive techniques. For this reason, the factors influencing wildfire prevention strategies in Cyprus were investigated to provide a comprehensive list of suggestions for improvement.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme MSCA-ITN-2019- Innovative Training Networks under grant agreement No. 860787. We would also like to extend our thank to Isabeau Romaine Ottolini and Kathleen Uyttewaal for their constant support during the preparation of this paper.

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.

RESPOND-A

New Technologies to Improve First Responder Safety – RESPOND-A Project

George Boustras[1], Cleo Varianou-Mikellidou[2], Iason Senekkis[3]

1. Professor in Risk Assessment, European University Cyprus
2. Lecturer in Occupational Safety & Health, European University Cyprus
3. Research Associate, CERIDES – European University Cyprus

1. RESPOND-A Project Description

With the evolving threat of climate change and the consequences of industrial accidents becoming more severe, there is a growing need for First Responders (FRs) to have access to reliable and flexible information management systems that offer better situational awareness and a better common operational picture. Considering this need, the European project RESPOND-A aims to develop holistic and easy-to-use solutions for FRs.

RESPOND-A introduces a unique five-tier project architectural structure for best associating modern telecommunications technology with novel practices for FRs of saving lives, while safeguarding themselves, more effectively and efficiently. The introduced architecture includes Perception, Network, Processing, Comprehension, and User Interface layers, which can be flexibly elaborated to support multiple levels and types of customization, so as, the intended technologies and practices can adapt to any European Environment Agency (EEA)-type disaster scenario.

The objectives of RESPOND-A are:

- To identify the Situational Awareness requirements of FRs and specify how the proposed mission-critical networks and applications can reflect these requirements in cost-effective and Social, Ethical, Legal, and Privacy (SELP)-aligned manner.
- To develop and provide to FRs equipment tools with continuous connectivity for protecting them against multiple unexpected dangers, and facilitate their operations by upgrading the Common Operational Picture (COP) and Situational Awareness.
- To deploy and use on demand connected fleets of UAVs for improving personnel safety and ensuring seamless access to video and sensor data for all types of FRs involved in the project.
- To extract knowledge and directions for training exercise of FRs with respect to the usability of the proposed tools and applications, so as, each end-user can be fully familiarized with these new technologies.
- To deploy on site and in position experimental testing and perform real-world validations of the developed network-enabled equipment tools and applications using the training facilities available by our Responder Partners.
- To execute large-scale demonstration at the Port of Valencia, based on concrete application scenarios for Police, Fire Fighters, EMS, and pilot cases, targeting to a COP. After the demo, provide evaluation reports and references.
- To design and establish novel practices for the interaction between FRs and research centres, so as, the newly introduced network tools and applications will be easily understood and smoothly incorporated.
- To disseminate and communicate the project technological, conceptual and practical outcomes for raising impact awareness on Responder organisations and the wider community, and exploit synergies with other EU projects.
- To provide an exploitation strategy and develop a business marketing plan for the potential commercial rollout of the RESPOND-A project results, either as a whole solution or partial components.

RESPOND-A seeks to promote the development of technologies based on 5G wireless communications, augmented and virtual reality or autonomous robots to optimize the work of FRs.

The technologies have been used in pilot exercises and trainings to ensure their quality. Through the use of smart portable sensors that record and measure data related to the operational environment, but also give information about the health status of the FRs Responder, the Command and Control Centers can have a complete picture of the safety status of the FRs and their surroundings.

The scope of the project is the development of upgraded communication tools and devices for FRs, i.e. for Emergency responders in cases of natural and man-made disasters. The Emergency Responders have real-time access to important data sources through the equipment that enables them to analyse the risk and draw up plans. All innovative products developed will enable FRs to collaborate in a safer and more efficient way, increasing the safety and effectiveness of the response to various incidents. Throughout the project's duration, the conclusion is that health and safety

challenges of FRs can be addressed by implementing new technological solutions. The total project budget is 7.67 million euros. It brings together 33 organizations from 13 European countries. Among them research centers, universities, private organizations and government agencies. The project is coordinated by the European University through CERIDES (Center of Excellence in Risk and Decision Sciences).

Acknowledgements
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883371. 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.

SAFERS

SAFERS: Structured Approaches for Forest fire Emergencies in Resilient Societies

Edoardo Arnaudo[1], Luca Bruno[1], Federico Oldani[1], Marko Laine[2], Conrad Bielski[3], Alberto Croci[4], Andrea Trucchia[5], Panagiota Masa[6], Mike Payne[7], Claudio Rossi[1]

1. LINKS Foundation, AI, Data & Space (ADS)
2. Finnish Meteorological Institute (FMI)
3. Riscognition GmbH
4. WaterView s.r.l.
5. CIMA Research Foundation
6. Centre for Research and Technology Hellas (CERTH)
7. Astrosat Ltd.

Forest fires have been a growing concern due to the increasing frequency and magnitude of extreme weather conditions exacerbated by climate change. This global issue has resulted in the loss of human lives, habitats and the emission of millions of tons of CO2 and other pollutants. Therefore, it is critical to have effective forest fire emergency management systems to limit future events' impacts.
The SAFERS project (Structured Approaches for Forest fire Emergencies in Resilient Societies) addresses this challenging issue by proposing a comprehensive Emergency Management System (EMS) to manage forest fires across all key phases of the emergency management cycle.
SAFERS leverages a service-oriented approach to integrate a set of Intelligent Services (IS) based on different data sources, including Earth Observation from the EU Copernicus program, meteorological forecasts, hazards and risk forecasts, propagation models, crowdsourced data from social media and ad-hoc mobile applications, and real-time data from in-situ cameras sensors. The outputs of the SAFERS IS are stored within a geospatial Data Lake, harmonized, and presented to the end users through an interactive web-based dashboard to enable better-informed decision-making along the entire emergency management cycle.

Deterministic and probabilistic weather forecasts, fire hazard, susceptibility (e.g., FWI) and risk predictions are processed by a rule-based Decision Support System that can be configured to generate CAP-compliant early warnings in the preparedness phase. Optical images from low-cost in-situ cameras are processed using advanced algorithms based on Artificial Intelligence (AI) to detect smoke or flames, estimating the distance from the observation point and the location of the detected fire event. After detection, a real-time alert will be sent to timely inform end-users. During the response phase, a probabilistic propagation algorithm [1] can estimate the forest fire temporal evolution (i.e., fire isochrones) based on several factors, including the forecasted weather and soil conditions (e.g. the wind speed and direction, the soil humidity) as well as the fuel map. The model stochastically propagates the fire boundaries using a cellular automata algorithm, starting from the provided initial conditions. The predicted fire propagation algorithm also outputs the mean and max fire intensity and rate of spread. First responders can use such information to define the best fire suppression strategy while ensuring the safety of the deployed forces. After the event, satellite data from Copernicus (mainly Sentinel-2) are exploited with supervised deep learning models based on Convolutional Neural Networks (CNN) [2] [3] to enable the automatic mapping of burned areas, delivering a burned severity index together with the list of impacted elements. To extract the affected population, infrastructures, and land, the JRC Global Human Settlement Layer, Open Street Map, and the CORINE land cover are used, respectively. Moreover, SAFERS allows the monitoring of soil recovery, providing maps containing the temporal evolution of vegetation indexes (e.g., NDVI). Delineation and severity estimate algorithms exploit Convolutional Neural Networks (CNN) to segment the areas affected by wildfires.

At all phases, the crowdsourcing service enables the exploit citizen-generated data. On the one hand, the social media data engine gathers and classifies Twitter posts in real time, automatically discarding uninformative or irrelevant content. This service exploits Natural Language Processing (NLP) [4] and clustering techniques to detect emergency events [5], estimating their impacts in terms of affected people and infrastructures using a rule-based approach [6]. On the other hand, end-users such as first responders and volunteers can provide structured geolocated and multimedia data through a Telegram Chatbot, which also enables to manage missions and receive georeferenced communications created in the SAFERS dashboard.

The overall architecture is shown in Figure 1. The central backend is the core building block of the system, orchestrating the communication between modules. Most of the interaction with Intelligent Services is asynchronous and event-based: map requests are forwarded through the bus on demand, the recipient service provides updates on the process, and uploads the results onto the Geo-Data Repository. Periodical data such as weather forecasts are instead directly pushed to the data lake, without user interaction. Every dataset must have INSPIRE-compliant metadata, and is automatically imported, mapped, and made available to the dashboard via OGC protocols (WMS or WTMS). Other services (e.g., crowdsourcing solutions) may also directly provide data through standard REST API for direct visualization.

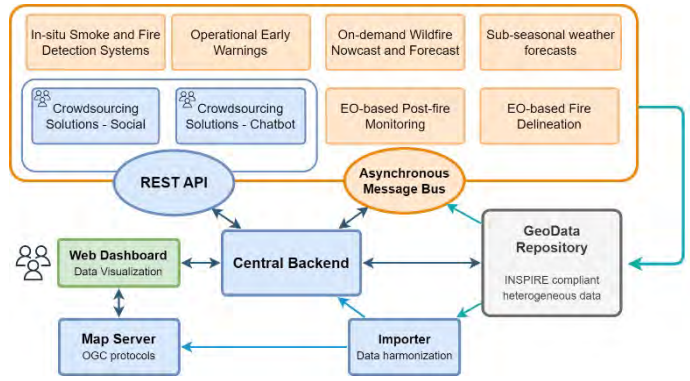


Figure 1. *Overview of the SAFERS architecture.*

Acknowledgements

This project has received EU funding through the SAFERS project (grant agreement No. 869353).

References

[1] A. Trucchia, M. D'Andrea, F. Baghino, P. Fiorucci, L. Ferraris, D. Negro, A. Gollini and M. Severino, "PROPAGATOR: An operational cellular-automata based wildfire simulator," Fire, vol. 3, p. 26, 2020.

[2] A. Farasin, L. Colomba and P. Garza, "Double-step u-net: A deep learning-based approach for the estimation of wildfire damage severity through sentinel-2 satellite data," Applied Sciences, vol. 10, p. 4332, 2020.

[3] F. Montello, E. Arnaudo and C. Rossi, "MMFlood: A Multimodal Dataset for Flood Delineation From Satellite Imagery," IEEE Access, vol. 10, p. 96774–96787, 2022.

[4] S. Piscitelli, E. Arnaudo and C. Rossi, "Multilingual text classification from twitter during emergencies," in 2021 IEEE International Conference on Consumer Electronics (ICCE), 2021.
[5] D. Salza, E. Arnaudo, G. Blanco and C. Rossi, "A'glocal'approach for real-time emergency event detection in twitter," in ISCRAM 2022 Conference Proceedings-19th International Conference on Information Systems for Crisis Response and Management, 2022.
[6] G. Blanco, E. Arnaudo, D. Salza and C. Rossi, "Impact Estimation of Emergency Events Using Social Media Streams," in 2022 IEEE 7th Forum on Research and Technologies for Society and Industry Innovation (RTSI), 2022.

Search & Rescue

Search and Rescue

The Search and Rescue Project: Emerging Technologies for Early Location of Entrapped Victims under Collapsed Structures and Advanced Wearables for Risk Assessment and First Responder Safety in SAR Operations

Sofia KARMA[1], Christos NTANOS[1]

1. National Technical University of Athens

1. Introduction

Extreme weather events currently observed on a global scale have been correlated with the current "climate crisis", which, combined with population growth and urbanisation, has exacerbated the consequences in terms of disaster casualties, property losses, and environmental impacts. The Search and Rescue project, among other related initiatives, has implemented part of the Disaster Risk and Resilience priorities outlined in the UN's 2030 Sustainable Development Agenda. Its primary goal was to establish and promote a comprehensive framework encompassing system and equipment interoperability, training, and awareness by providing cutting-edge technologies and innovative tools for the first responders.
The technologies, tools, and techniques developed within the Search and Rescue project were successfully tested and validated through seven field exercises based on various use-case scenarios. Within this framework, a promising field technology – Membrane Inlet Mass Spectrometry (MIMS) – was adapted to meet the needs of first responders and tested for the first time in search and rescue operations with the 'RESCUE-MIMS' prototype (TRL 6). Specifically, the device was used in relevant exercises and tested a) as an early warning system on-board a ground robotic platform for first responders' safety, and b) as an "artificial sniffer" for detecting compounds related to human presence according to literature, complementing rescue dogs.

2. Methodology

It is important to point out that mimicking rescue dogs in a disaster scene is a complex issue since hundreds of chemical compounds with different origins can be present. In Figure 1, testing of the RESCUE-MIMS in the field under the scenario "People Trapped Under the Rubbles" that took place in Limoges, France in cooperation with the PUI team (Pompiers de l' Urgence Internationale), is shown.

Figure 1. *Testing of the RESCUE-MIMS in the field under the scenario "People Trapped Under the Rubbles" that took place in Limoges, France in cooperation with the PUI team*

Based on the scenario, the RESCUE-MIMS device was deployed in the field for measuring the compounds inside the voids of the collapsed structure and for providing a possible "alarm of a human" under the rubbles.

3. Results

The RESCUE-MIMS was able to successfully detect online the increased intensities of masses that are correlated with compounds relevant to human exhaled air according to the literature, like Carbon Dioxide and Acetone, compared to the background measurements recorded inside the voids (See Figure 1). The RESCUE-MIMS was also used in another use case inside the Search and Rescue project (forest fire expanded and threat an industrial zone), and tested as an early warning system onboard a ground robotic platform for the first responders' safety; hazardous compounds, such as ammonia (NH3), carbon monoxide (CO), Benzene, were successfully monitored on-line and the respective alarms were sent to the SnR platform at the command and control center.

Specific Key Performance Indicators (KPIs) were used to evaluate the RESCUE-MIMS prototype in the aforementioned use cases; portability; robustness; easiness to operate; easiness to deploy; friendliness to the user; fast response times; high sensitivity; minimum false positives/negatives. Also, it has to be mentioned that in both use cases usability testing of the Rescue MIMS prototype took place with the assistance of the end-users. An important consideration when measuring online in the field is the potential background interferences that may create false positives or negatives; for this reason, background measurements were recorded by the RESCUE-MIMS in the respective pilots.

Conclusions

Based on the first responders' feedback, it became apparent that it was possible to use a highly sensitive analytical technique in terms of ultra-low detection capabilities with minimum false alarms alongside sophisticated analytical equipment in the field. It is a promising field technology that can be used as a complementary tool to the classical detection options for location of entrapped victims under collapsed structures, in order to help the first responders in search and rescue operations, e.g. to cope with limitations when using rescue dogs in terms of availability, fatigue or incomplete/insufficient training. The RESCUE-MIMS technology has proven its effectiveness, but there is still room for improvement in terms of weight, ease of use, resistance to environmental, field conditions and operating autonomy. Also, special training is needed by the users, e.g. one or two members from the firefighters team should be trained every 2-3 months, as already do for similar technologies, like the scanner or the drones.

Acknowledgements

The Search and Rescue project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 882897. 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.

SEARCH AND RESCUE: EMERGENCY TECHNOLOGY FOR FIRST RESPONDERS

Izquierdo Funcia S[1], Aldea Reyes A.M.[1], Burgos Gonzalez M.[1]

1. Spanish School of Rescue & Detection Dogs (ESDP)

The Search and Rescue (SnR) project was launched on 1 July 2020, funded by the European Commission under grant agreement 882897. Its main objective is to develop technologies that help emergency teams to reduce search and rescue times for victims in disaster situations. ESDP collaborates with companies from countries belonging to the European Union, forming a consortium that seeks to develop technologies that improve the detection of risks, the collection of data from the disaster area, as well as the processing and optimization of the use of this data. The goals were as follows:

• Optimization in the flow of information.
• Reception and management of information from emergency teams in real time.
• Development of tools capable of reflecting the situation in the disaster area.
• Communication platforms, personal location and information gathering from different devices, together with the IT architecture capable of supporting all these elements will be responsible for the success of this project.
• Localization systems for rescue dogs, which determines the location of the victim through GPS coordinates immediately and its automatic registration in the platform.
• One of the most innovative points of this project is the development of localisation systems for rescue dogs, which allows the location of the victim to be known immediately through GPS coordinates and their automatic registration on the platform.

From the beginning of the SnR project, the requirements of first responders as end-users have been taken into account through different qualitative and quantitative research tools (workshops, interviews and questionnaires). Emergency, search and rescue experts and technology developers have worked together to create innovative technologies that increase the safety of first responders and reduce the rescue time associated with responding to different types of emergencies in challenging. One of the most important phases of the project has been to implement and evaluate the general approach of the S&R platform and to define the validation activities in order to ensure the relevance of the results in terms of scientific and technical objectives. These activities were integrated into various use cases where emergency situations were reproduced to test the capabilities of these technologies to response the following scenarios.

- UC1: Victims trapped under rubble (Italy)
- UC2: Air crash, mountain rescue, non-urban (Greece)
- UC3: Earthquake / strong storms between Vienna train station and Kufstein train station, severe damage to train station (cross-border pilot, Austria-Germany)
- UC4: Expansion of forest fire and threat to industrial area (Attica region, Greece)
- UC5: Victims trapped under the rubble (France)
- UC6: Supporting resilience of critical infrastructures through standardised CBRN training (Romania)
- C7: Chemical spills (Spain).

The fusion of different sources to create a common analysis of the situation provides us with a "bird's eye view" of the advanced procedures that will help us to achieve the highest level of disaster response capability:

• Development of an IT architecture for data collection and circulation.
• Fusion of different sources to create a common analysis of the situation.
• Creation of a global vision of the disaster scenario.

Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 882897.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.

SILVANUS

EU sustainable forest management and wildfire policies and practices: Challenges between "As Is" and "To Be" state

Nikolaos Kalapodis[1], Georgios Sakkas[1], Miltiadis Athanasiou[1], Dimitrios Sykas[2], Konstantinos Demestichas[2], Spyridon Kaloudis[2], Alexandre Lazarou[3] and Domenica Casciano[3]

1. Center for Security Studies (KEMEA)
2. Agricultural University of Athens (AUA)
3. Zanasi Alessandro SRL (Z&P)

As Is: Climate change has been a major factor in increasing the risk and impact of wildfires in Europe in recent decades, with far-reaching implications for the environmental, social, and economic conditions, as well as for essential ecosystem services provided by forests. Wildfires have multiple impacts, including:

- loss of human lives, injuries as well as short and long-term health effects,
- burning of large-scale forest areas, emission of millions of tonnes of carbon dioxide and smoke particles, degradation of soil and downstream water quality, increasing flood risk, disruption of wildlife habitats, environmental pollution, loss of biodiversity, etc.,
- damage to buildings, infrastructure, agricultural cultivations and livestock facilities, significant losses of timber and non-timber products, impacts to tourism, carbon sinks, reduced protection of agricultural soils, aquifers and biodiversity causing significant financial losses per year over Europe and
- recreational activities, loss of aesthetic values, psychological impacts, educational activities, etc.

The Intergovernmental Panel on Climate Change (IPCC, 2021) reports that the rise of temperatures in Europe will continue at a rate exceeding the global mean temperature change, that has already reached 1.1°C above pre-industrial levels (IPCC, 2023). Apart from the secondary effects of the phenomenon of climate change (pest and diseases, insect calamities, and wind-throws) in central and northern Europe, the risk of large and uncontrolled wildfires is likely to increase in these two regions of the world, which until recent decades have been less prone to wildfires (Khabarov et al., 2014). Moreover, according to Lindner et al. (2014), climate change projections for the Mediterranean region also indicate that extremely dry years will become more frequent and droughts much longer in the future. The EU is working on measures to mitigate the impacts of forest fires and published the EU Strategy on Adaptation to Climate Change. **To Be:** The strategy emphasises that adaptation needs to be faster, smarter, and more systemic, and to step up international action on adaptation to climate change. Also, the guidelines on land-based wildfire prevention by the European Commission, Directorate-General for Environment (Nuijten et al., 2021) call for managing vegetation and avoiding the accumulation of fuels on the ground to facilitate firefighting.

In addition, the new EU Forest Strategy for 2030, adopted by the European Commission, is one of the flagship initiatives of the European Green Deal and builds on the EU Biodiversity Strategy for 2030. **To Be:** The strategy sets out a vision and concrete actions to improve the quantity and quality of EU forests and to strengthen their protection, restoration, and resilience through sustainable forest management (SFM).

The European Commission's proposal for a Nature Restoration Law is the first continent-wide, comprehensive law of its kind. It is a key element of the EU Biodiversity Strategy, which calls for binding targets to restore degraded ecosystems, in particular those with the most potential to capture and store carbon and to prevent and reduce the impact of natural disasters. **To Be:** The proposal aims to restore ecosystems, habitats and species across the EU's land and sea areas in order to enable the long-term and sustained recovery of biodiverse and resilient nature, and to contribute to achieving the EU's climate mitigation and adaptation objectives meet international commitments.

Challenges: This research followed a twin-tracked approach, based on extensive published literature reviews, through desk research, and primary research with relevant experts and stakeholders using designed questionnaires on the above-mentioned specific fields. The purpose is to discuss forest management and wildfire policies and practices, to identify potential challenges (gaps and potential conflicts) related to wildfire prevention and restoration.

Recent findings: The role of forest ecosystem is discussed, in conjunction with EU policies to address climate crisis, including the EU Green Deal and wildfire policy. The study presents SFM as a holistic approach, as well as the principles of closer-to-nature forest management. Post-fire forest restoration is also discussed, including pre- and post-fire impact assessment.

Acknowledgements

This study has been conducted in the framework of 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.

SILVANUS

Measuring Forest Resilience against Wildfires and Climate Change – Methods and Technical Approaches

Konstantinos Demestichas[1*], Dimitrios Sykas[1], Dimitrios Zografakis[1], Spyridon Kaloudis[2], Nikolaos Kalapodis[3], Georgios Sakkas[3], Miltiadis Athanasiou[3], and Constantina Costopoulou[1]

1. Department of Agricultural Economics and Rural Development, Agricultural University of Athens
2. Department of Forestry and Natural Environment Management, Agricultural University of Athens
3. Center for Security Studies (KEMEA), Ministry of Citizen Protection

Forest resilience against wildfires and climate change refers to the capacity of a forest ecosystem to withstand and recover from the combined impacts of these two types of disturbances. In this context, forest resilience involves the ability of a forest to withstand the increased frequency and severity of wildfires that can occur due to changing climatic conditions, such as drought and heatwaves, adapt to changing environmental conditions, such as shifting temperature and precipitation patterns, and changes in the distribution of species and communities, maintain its ecological functions and services, such as carbon sequestration, biodiversity conservation, and water regulation, even under changing conditions, recover effectively from wildfire and other disturbances, by regenerating forests, supporting post-fire ecosystem processes, and reducing the risk of future fires (Falk et al, 2022).
Measuring and assessing forest resilience to wildfires and climate change involves both quantitative and qualitative methodologies. Quantitative methods focus on measuring specific ecosystem parameters that affect a forest's ability to recover from a wildfire, while qualitative methods aim to understand the social and ecological factors that contribute to a forest's resilience.
Qualitative methodologies include: Social and ecological surveys: Surveys of local communities and stakeholders can provide insights into the social impacts of a

wildfire and the factors that contribute to a forest's resilience. **Stakeholder engagement:** Engaging with stakeholders, such as local communities, indigenous peoples, and forest managers, can help to understand the social and ecological factors. Participatory mapping: Participatory mapping exercises can help to identify areas of high ecological and cultural value, which can inform restoration and management strategies. Expert elicitation: Expert elicitation techniques, such as workshops and interviews with forest managers and researchers, can provide insights into the ecological and social factors that contribute to a forest's resilience and inform management and restoration strategies.

Quantitative methodologies (Schmidt et al, 2022) include: Vegetation monitoring: Monitoring changes in vegetation, such as plant cover and species composition, can provide insights into the recovery of the ecosystem after a wildfire. The vegetation monitoring can be addressed with different technical means, depending on the specific objectives of the action (ground observations, drones, satellite imaging). Ground observations monitoring can provide important information on plant density, height, and other quantitative measurements that can help assess changes in vegetation after a wildfire. They are generally considered as a more accurate and detailed form of vegetation monitoring, compared to remote sensing methods, although they may be less efficient for covering large areas. Soil sampling: Sampling soil after a wildfire can help to assess changes in soil fertility, organic matter content, and nutrient cycling, which can affect the ability of vegetation to regrow. Hydrological monitoring: Monitoring changes in water availability and quality can help to understand the impacts of a wildfire on the water cycle and the potential for erosion and landslides.

The use of Earth Observation (EO) is one of the most important quantitative methods for measuring and supporting forest resilience, by monitoring changes in forest health, identifying areas of risk, and informing management strategies. EO data for measuring forest resilience include: Optical imagery: Optical satellite imagery can be used to monitor changes in forest cover, including the extent of deforestation, forest fragmentation, and the impacts of natural disturbances, such as wildfires and climate change, as well as to monitor forest health, including changes in tree canopy cover and the presence of diseases or pests. LiDAR data: LiDAR (Light Detection and Ranging) is a remote sensing technology that can be used to measure forest structure and biomass. LiDAR data can be used to create detailed 3D models of forest ecosystems, providing valuable information on forest health and productivity. Radar data: Radar data can be used to monitor changes in forest cover and structure, including the detection of forest disturbance and the mapping of forest biomass. Radar data can also be used to monitor changes in soil moisture levels, which can affect forest health and resilience. Climate data: Climate data can be used to assess the potential impacts of climate change on forest ecosystems, including changes in temperature, precipitation, and extreme weather events. Also, they can be used to model future forest growth and productivity under different climate scenarios. Topographic data: They can be used to identify areas of risk for natural hazards, such as landslides and floods, as well as areas of high biodiversity.

Acknowledgements

This study has been conducted in the framework of 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 EC.

References

1. Falk, D. A., et. al. (2022). Mechanisms of forest resilience. Forest Ecology and Management, 512, 120129. doi: 10.1016/j.foreco.2022.120129
2. Schmidt A., et. al. (2022). A quantitative wildfire risk assessment using a modular approach of geostatistical clustering and regionally distinct valuations of assets—A case study in Oregon. PLOS ONE 17(3): e0264826. doi: 10.1371/journal.pone.0264826

Integrated fire management system for delivering holistic capability to combat against wildfires

Michele Corleto[1], Lovorko Maric[2], Krishna Chandramouli[3]

1. Department of Law, Università Telematica Pegaso
2. Micro Digital
3. Venaka Treleaf GbR

Abstract:
Globally, wildfires and volcanic activities affected 6.2 million people between 1998-2017 with 2400 attributable deaths from suffocation, injuries, and burns, but the size and frequency of wildfires are growing due to climate change1. Hotter and drier conditions are drying out ecosystems and increasing the risk of wildfires. Wildfires also simultaneously impact weather and the climate by releasing large quantities of carbon dioxide, carbon monoxide and fine particulate matter into the atmosphere. Resulting air pollution can cause a range of health issues, including respiratory and cardiovascular problems. Another significant health effect of wildfires is on mental health and psychosocial well-being. Addressing such challenges, the SILVANUS2 project aims to deliver an environmentally sustainable and climate resilient forest management platform through innovative capabilities to prevent and combat against the ignition and spread of forest fires. The platform will cater to the demands of efficient resource utilisation and provide protection against threats of wildfires encountered globally. The project will establish synergies between (i) environmental; (ii) technology and (iii) social science experts for enhancing the ability of regional and national authorities to monitor forest resources, evaluate biodiversity, generate more accurate fire risk indicators, and promote safety regulations among citizens through awareness campaigns.

1. Introduction

The future of wildfire prevention, detection and response will be defined by further development of technological innovation and a well-organised coordination between on-site data acquisition and efficient interpretation. This will increase the reliability of wildfire prevention systems. Since the wildfire phenomenon is becoming an increasing threat in the climate crisis of today, an integrated technological solution incorporating all vital technological and information components is therefore crucial. The SILVANUS project proposes the implementation of an environmentally sustainable integrated technological platform for wildfire management, which includes IoT fire detection and edge computing as essential components in wildfire management. The platform will facilitate quicker response times to a wildfire threat, enable higher reliability of data, and make data interpretation more efficient. This paper will elaborate how deployment of IoT fire detectors and development of edge computing will enhance the data collection and processing to make extreme wildfire prevention and suppression more effective and sustainable.

2. Innovation

The design of the SILVANUS platform addresses the modelling of ecological environment for sustainable forest management requires the development of structured knowledge models that support the collection and formalisation of a biodiversity profile for a specific geographic region. Changes in biodiversity are due to three basics ecological processes: 1) invasion of exotic plants, 2) progressive succession as a part of the ecological process, and 3) retrogressive succession due to natural and anthropogenic pressures on ecosystems. Assessment of changes in biodiversity or the state of biodiversity will be evaluated using functional traits and groups along with structural indicators such as Essential Biodiversity Variables (EBV). Studies by Nally and Fleishman have shown that identification and analysis of the behaviour of relatively few indicator species in a community can predict the variation in 89% of the species in the community. The SILVANUS project has undertaken investigation into the development of a biodiversity index, by building a crowd sourced mobile application for collecting tree species and using AI to automatically classify and categorise the relevant information known as the FIPAS application.
Towards raising awareness about the impact of wildfires, the project has developed a citizen science programme to engage with diverse communities and avail the effectiveness of semantic technologies to facilitate knowledge sharing among stakeholders. The knowledge developed in the project will be used to enhance preparedness for combating wildfires, response coordination and rehabilitation activities. The development of an advanced semantic engine component will build on the

ontology structure and will facilitate multi-lingual representation of biodiversity and ecological analysis models. The human factor consideration will include the impact of negligence and the ability to share information on the identification of safety violations. The project has integrated the use of data-driven AI approaches to develop the wildfire spread model, along with statistical tools developed for assigning the fire danger risk index. Lastly, the sustainable forest management toolkit will leverage the knowledge gathered on the geographical context to build advanced visualisation maps for both training activities and scenario planning along with the deployment of technologies to detect wildfires. Additionally, the use of onboard data analytics with low-cost computational components capable of performing video stream analytics at the edge will extend the longevity of the drone flight time. Complementing the edge computing capability, the use of Earth Observation data analytics supported using Copernicus dataset will be subsequently analysed in the cloud using big-data framework integrated with data fusion components.

3. Pilot demonstrations

Pilot demonstrations: The evaluation and validation of the SILVANUS platform will be carried out through the deployment of technological solutions on the field. To this end, the project has undertaken two pilot exercises, in April 2023, as indicated below. The pilot demonstration brought together the stakeholders represented by forest management authorities, public administration bodies, fire fighters

4. Conclusion

The proposed novelty of the platform will be validated by adopting evidence-based approach and demonstrating the impact of AI and other tools for combating against wildfires. Further pilot activities have been rganized to be carried out in Greece, Portugal, Romania, Italy (Apulia, Sardinia), Czech Republic, and France during the Autumn period of 2023. The platform demonstration will integrate IoT devices, drones, robots, Earth Observation data sources, weather and climate data services, and other sources.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement for SILVANUS project No. 101037247. 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://www.who.int/health-topics/wildfires#tab=tab_1
2. https://silvanus-project.eu/

STRATEGY

Resilient infrastructures through (pre-) standardization: The STRATEGY Perspective

Ioannis Chasiotis[1], Georgios Sakkas[2], Danai Kazantzidou-Firtinidou[2], Aikaterini Valouma[1], Leonidas Perlepes[1], Nikolaos Stefanou[3], Ilias Gkotsis[1], Aikaterini Poustourli[1]

1. Satways Ltd
2. Center for Security Studies (KEMEA)
3. Hellenic Police, Joint Coord. Cent. for Operations & Crisis Management

Nowadays, threats and hazards being faced by Critical Infrastructures (CIs) become more frequent and complex, underlining the need for effective crisis management processes across all phases of the respective cycle. Standardised practices for preparing, responding, and mitigating the onset and results of such crises will enhance the efficiency of crisis management and improve the overall resilience of the CIs.
In the framework of STRATEGY project, pre-standardisation tasks addressing interoperability-related issues for systems / procedures across relevant thematical domains of crisis management, were undertaken. This paper analyses a proposed approach for improving the resilience of CIs considering interrelated pre-standardisation outcomes (CEN Workshop Agreements-CWAs) as developed by STRATEGY project.
Reliable rapid damage assessment reports shared with CIs and first responders, incident notification and situational awareness reports, communication and sharing of information among multiple emergency services leveraging on aligned emergency response planning practices with homogeneous training based on structured evaluation practices, support the enhancement of interoperability across all levels (cross-level, cross-organization, cross-border). The combined result of such actions, as addressed through pre-standardisation within STRATEGY, facilitates the establishment of resilient CIs, improved services, and mitigation of impacts, including loss of lives and economic losses. Produced outcomes were validated through sustainable tests, exercises and evaluation frameworks, for ensuring reliable results that will upgrade the crisis management and disaster resilience capacity.
Provided the above, the authors propose a mechanism of interoperating pre-standardization items that can be applied to a CI incident, across primarily the preparedness, response and mitigation phases of the disaster management cycle, each contributing to the overall enhancement of resilience as outlined below.

• Perform Rapid Damage Alerting upon the onset of a disastrous event.

Public services and practitioners must be alerted as rapidly as possible on damaged buildings and infrastructures to act promptly and in a targeted manner.
This need is partially related to the operational requirement to share information on disaster damages among a significant number of public services involved in mitigation, response, and recovery activities. Damage should sometimes, nonetheless, be estimated in near-real time / real time following the incident, and automatically reported to the appropriate authorities. Therefore, to maximize the effectiveness and efficiency of public safety agencies, a formalized method for sending alerts describing potential damage is proposed [1].

• Provide accurate incident reports and notifications for CIs.

Incidents affecting CIs can have a significant impact on the provision of vital services in society. STRATEGY proposes a new structured approach of requirements and recommendations for CIs w.r.t. incident reporting and notification [2]. The overall approach considers existing knowledge from various types of stakeholders and relevant standards (OASIS EDXL SitRep, M/ETHANE, ISO/TR 22351) that can lead to the improvement of resilience. Moreover, this approach could also support the adoption of the EU 2557/2022 CER Directive from Member States.

• Establishment of homogeneous response planning approaches

In the case of disastrous events involving CIs, successful response usually entails the efficient coordination of a multi-stakeholder environment (e.g. infrastructure operators, first responders, local governments, public etc.). STRATEGY project has proposed an approach for enhancing interoperability through homogenizing the structure of response plans for each organization – thus (among others) facilitating the process of exchanging information during operations [3]. A template consisting of a set of sections along with respective guidelines for assisting planners to establish their plans is being pre-standardized.

• Improving collaborative response through a common addressing format and emergency identification protocol.

Communication and cooperation between public and private safety organizations is essential during an emergency involving CIs. Public safety agencies engaged in large-scale, and extensive situations of this category may originate from different countries. To facilitate collaboration and sharing of operational information, these agencies usually exploit digital means (e.g., incident management systems). The effectiveness of the collaboration is limited by the absence of a common inventory for hosting and routing each agency's information sharing provisions. STRATEGY suggests a standard method for centrally routing the respective information among emergency agencies across the EU.

• Management of wildfire incidents using SITAC-based symbology

Information related to the characteristics of the area of operations in case of wildfire incidents affecting CIs, the evolution of the fire, intervention measures, and current or planned response actions is encompassed by the proposed SITAC-based symbology. The proposed method consists of a set of symbolic icons designed to be used with paper and digital maps. The envisaged standardization will support the onsite coordination of wildfires response, through enhancing communication and cooperation among the firefighting organizations and actors involved.

• Establish a uniform training framework for optimizing response.

Exercises as a technique of experiential training and learning need to be conducted at national, regional, or organizational level, primarily aiming to the enhancement of operational capabilities and the strengthening of collaborative response capacity. Exercises for CI Protection aim to a) increase awareness on interdependencies and involved stakeholders, b) estimate impact from service disruption and anticipation of prevention measures, as well as c) enhance joined response capacity among emergency responders and involved operators [4]. The CWA as proposed by STRATEGY aims to further improve the evaluation schema and the elaboration of concise documentation of exercises outcomes. These are directly addressed to exercise managers and lead evaluators of any organization that envisions planning, conducting and reviewing exercises in a homogenized manner.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883520. 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. Aikaterini Valouma, Leonidas Perlepes, Ioannis Chasiotis, et al. "Critical Infrastructure Protection: Standardisation and Exercises" - 9th International Conference on Civil Protection & New Technologies, Sept 2022, Thessaloniki – Greece, Proceedings | ISSN 2654-1823

2. Georgios Sakkas, Danai Kazantzidou-Firtinidou, Ioannis Tsaloukidis, et al. "Critical Infrastructure Protection: Standardisation and Exercises" - 9th International Conference on Civil Protection & New Technologies, Sept 2022, Thessaloniki – Greece, Proceedings | ISSN 2654-1823

3. Ioannis Chasiotis, Nikolaos Stefanou, George Sakkas et al. "Emergency Response Planning: Efficiency through Standardization" - 9th International Conference on Civil Protection & New Technologies, Sept 2022, Thessaloniki – Greece, Proceedings | ISSN 2654-1823

4. Stefanou, N., Kazantzidou-Firtinidou, D., Sakkas, G., Theodoridis, G., Rousakis, V. (2021). "Training and exercises for the protection of CIs – a Hellenic Computer-assisted use case analysis", International Journal of Disaster Risk Reduction 69 (2022) https://doi.org/10.1016/j.ijdrr.2021.102729.

STRATEGY
Interoperability for crisis management

The Data Governance Process within the Digital Chain of Custody

Gabriel Pestana[1], Luís M. Carvalho[2], Sebastian Chmel[3]

1. INOV - Institute of Systems and Computer Engineering Innovation
2. CINAMIL, AM, Instituto Universitário Militar / Unidade Militar Laboratorial de Defesa Biológica e Química, Exército Português,
3. Fraunhofer Institute for Technological Trend Analysis INT

Chemical, biological, radiological, nuclear, and explosive (CBRNE) incidents, whether caused by natural or accidental events or deliberate actions such as terrorism or warfare, typically require collecting and transporting samples to a laboratory for accurate identification of CBRNE agents. This process involves interactions among multiple stakeholders, making it essential to maintain the integrity of the chain of custody and document all actions to allow for auditing of the information flow, particularly at Custody Transfer Points (CTPs), to determine the involved stakeholders. This highlights the need for a digital chain of custody system that ensures the traceability and security of CBRNE evidence items throughout the entire process, including collection, transportation, analysis, and storage.

This document provides guidelines for the data governance workflow used to automate the digital custody transfer of digital evidence items, focusing on maintaining data integrity at each transfer point in the digital Chain of Custody (dCoC). The dCoC for CBRNE digital evidence is used as a case study to address data governance considerations for evidentiary purposes in a highly demanding framework. Within the dCoC data governance workflow, the integrity of the digital evidence must be preserved to ensure that even a single bit cannot be changed undetected. The dCoC data governance workflow should provide information about the digital evidence items and corresponding metadata, including who owns custody, how the custody transfer between stakeholders was accomplished, and the purpose of the transfer. Compliance with a consistent process is required to ensure the quality of digital custody metadata (DCM), which serves as a driver for stakeholders assuming custody of the evidence at each CTP.

The sensitivity and criticality of the data further underscore the importance of preserving the chain of custody, as this provides the necessary hallmarks of authenticity that the court increasingly demands. The document provides guidelines for managing and auditing DCM, enabling stakeholders to identify and audit custody ownership for CBRNE digital evidence items in the CTP lifecycle, raising awareness whenever an inconsistency is detected. A standardised approach with a well-defined DCM structure ensures that the digital evidence item can be considered relevant. The structure of the CTP data model used to characterise a digital evidence item should contain all the metadata needed to uniquely describe the data package transported from point A to point B. Fig. 1 provides a framework of the essential components that should be considered for the data governance of the stakeholders involved in a CTP, along with metadata to characterise the CTP lifecycle.

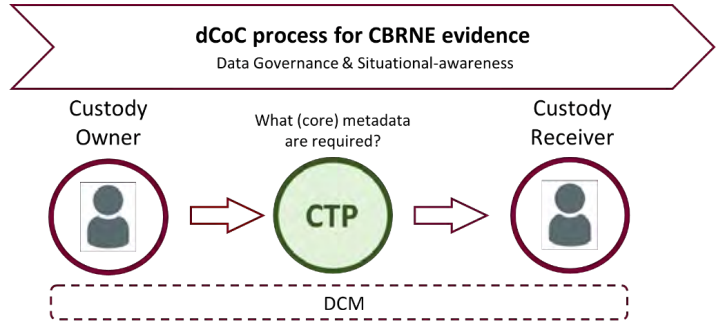


Fig.1. *Custody transfer schema within the dCoC process.*

The Business Process Model and Notation (BPMN) was adopted to specify the metadata management processes, providing a formal representation that helps understand the DCM-related challenges. The goal is to focus on the metadata structures required to manage digital asset custodians while outlining the data to be considered when specifying the data governance workflow. The BPMN diagram can improve the modelling of data governance for informational workflows and ensure that the dCoC supports and guides stakeholders' interactions with the system. The diagram provides a visual representation of the process, showing the steps involved and how they relate. This makes it easier for stakeholders to understand the process and identify potential areas for improvement.

Acknowledgements
The research presented in this paper was developed within the scope of the STRATEGY project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883250. The information presented in the paper was classified as public, it reflects a summary of the main achievements from the author's viewpoint.

Validation of Standardisation activities in Crisis Management through a Full Scale

Spyridon C. Athanasiadis[1], Panagiotis Michalis[1], Vangelis Tsougiannis[1], Eleftherios Ouzounglou[1], Lazaros Karagiannidis[1], Angelos Amditis[1]

1. Institute of Communication and Computer (ICCS)

1. Abstract

This study presents the validation activities carried out for two standardisation items entitled "Specifications for Digital Scenarios for Crisis Managements" [1] and "Requirements for acquiring digital information from victims during Search and Rescue operations" [2]. The results of the developments and the validation through a Full-Scale Exercise is presented which aims at collecting key feedback from participating crisis management stakeholders such us first responders, academia and researchers, industry and public authorities.

2. Validation of pre-standardisation activities in a full-scale exercise

The following two standardisation activities aiming to enhance interoperability in crisis management area were validated through extended Full-Scale Exercise carried out as part of STRATEGY project on the 30th March 2023 in Gualdo Tantino (Italy).

2.1 Digital Scenario Specifications for crisis management exercises

Technical and organisational interoperability in a fully transboundary configuration is considered of key importance [3,4]. However, the majority of crisis management exercises are following traditional approaches such as paper-based scenarios [5]. The development of a common data model for crisis management exercises was therefore considered of key importance and was the main focus of the first standardisation item presented in this study.
The FSX activities initially involved a roundtable with the participation of various stakeholders from different organisations. A presentation of the proposed data

model and a demonstration of the TMT execution manager was carried out, followed by a discussion focused on the evaluation of the CWA content for providing feedback. An example with respect to scenario planning as well as a short demonstration of the TMT execution manager were provided to participants, offering a better understanding of the proposed pre-standardisation activity also leading to fruitful discussions and collection of feedback by participants. The actual FSX then took place during which the content of the proposed CWA was put into practice incorporating two FSX scenarios which involved a large number of actors, events and injects. The execution of the virtual scenario was carried out by the TMT while certain injects that contained alarm messages were published to the message broker provided by the Driver+ framework [6] and then received by a Command and Control (C2) system.

2.2 Digital victim tracking system for mass casualty incidents

As healthcare resources are limited due to the number of injured individuals, digital victim tracking systems are implemented to offer the greatest good to the greatest amount of people [7,8]. The proposed CWA was tested in a FSX in the scenario of mass casualty incident where 65 victims and 70 first responders from different agencies involved. In total 70 triage tags used (20 digital victim tracking tags and 50 paper based with a QR code) and 370 transaction conducted between the tags and the mobile applications. All the tags scanned by the same mobile application by the first responders in 3 phases (primary triage, secondary triage and before dispatching to hospitals or after a major updated identified. The progress of the operation was available on the main platform (IN-SIDER) in real time shared with a C2 system.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883520, project STRATEGY. 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. CEN workshop Agreement 'Specifications for Digital Scenarios for Crisis Management Exercises', https://www.cencenelec.eu/news-and-events/news/2023/workshop/2023-03-23-digital-scenarios-for-crisis-management/
2. CEN CWA on Requirements for acquiring digital information from victims during Search and Rescue operations, https://www.cencenelec.eu/news-and-events/news/2023/workshop/2023-01-19-digital-information-search-and-rescue-operations/.
3. Michalis, P., Vintzileou, E. (2022). The Growing Infrastructure Crisis: The Challenge of Scour Risk Assessment and the Development of a New Sensing System. Infrastructures, 7, 68. https://doi.org/10.3390/infrastructures7050068
4. Michalis, P., Sentenac, P. (2021). Subsurface condition assessment of critical dam infrastructure with noninvasive geophysical sensing. Environmental Earth Sciences, 80, 556. https://doi.org/10.1007/s12665-021-09841-x.
5. Amditis A.J., Ouzounoglou E., Michalis P., Misichroni F., Perlepes L., Sdongos E. (2023) Interoperability and Standardisation Supporting Preparedness and Response to Disasters. Innovation in Crisis Management (eds Fonio, C., Widera A., Zwęgliński, T.) 1st Edition, Routledge, ISBN: 9781003256977, https://doi.org/10.4324/9781003256977
6. Driver+ (2020). Driving Innovation in Crisis Management for European Resilience (DRIVER+) (2020). Trial Guidance Methodology Handbook, 1st edition. https://tgm.ercis.org/fileadmin/user_upload/pdf/TGM_Handbook_EN.pdf
7. Misichroni F., Stamou A., Kuqo P., Tousert N., Rigos A. Sdongos E, Amditis A. (2021). A Novel, Reliable and Real-Time Solution for Triage and Unique Identification of Victims of Mass Casualty Incidents, Eng. Proc. 2021, 6, 72. https://doi.org/10.3390/I3S2021Dresden-10180
8. Rigos A., Sdongos E., Misihroni F., Stamou A., Kuqo P., Latsa E., Amditis A. (2019). A novel triage system using Bluetooth devices in support of incident management, 13th International Conf. on Sensing Technology (ICST), 10.1109/ICST46873.2019.9047744

VALKYRIES

Harmonization and Pre-Standardization of Equipment, Training and Tactical Coordinated Procedures for First Aid Vehicles Deployment on European Multi-Victim Disasters (VALKYRIES)

Yantsislav Yanakiev[1]

1. Bulgarian Defence Institute

Multi casualty incidents (MCI), where the number of victims far exceeds local resources and capabilities, are events that overwhelm the local healthcare system, at least for a period of time.

The response of the staff of the Emergency Medical Services (EMS) to these events often reveals insufficient resources (rescue personnel, medical personnel, facilities, etc.), communication difficulties and organizational interoperability problems with other first responders, which are more acute in cross-border, cross-sector and cross-hierarchical actions.

Echoing these needs, the project VALKYRIES (Harmonization and Pre-Standardization of Equipment, Training and Tactical Coordinated Procedures for First Aid Vehicles Deployment on European Multi-Victim Disasters) aims to develop, implement, validate and apply innovative theoretical foundations, methods, prototypes and their demonstration on a reference integration for supporting pre-standardisation and harmonisation of technologies, procedures, preparedness and cross-sector/border cooperation and training for first aid response in MCI.

The VALKYRIES project work has been split into seven work packages (WPs). Three of them (WP4, WP5 and WP6) focus on the three core blocks of working streams and have been developed in parallel: (a) Technologies and equipment: WP4; (b) Procedures and Operations: WP5 and (c) Collaboration and Training: WP6.

A common methodology was developed, agreed and used among the VALKYRIES WP4, WP5 and WP6 partners that was implemented at three steps. At the first step we analysed existing technologies, operative procedures and protocols, as well as preparedness and cross-sectorial collaboration opportunities for first aid response in cross-border MCI. The analysis is based on literature and documents review, subject matter expert's consultations and personal experiences of the VALKYRIES project partners.

The second step of VALKYRIES execution includes identification of the required capabilities for first aid responses by the end-users (first responders). Based on the study of the needs, the gaps between desired capabilities from those currently available were identified.

The next stage of the project implementation includes in-depth analysis and explanation of technological, procedural, collaboration and training capability gaps. As a result, a list of identified harmonization opportunities was created. After that, the VALKYRIES project partners analysed in depth all harmonisation opportunities to evaluate similarities and differences among them and to group the opportunities which cover the same or close topics. Accordingly, those opportunities that present common aspects were grouped/clustered, generating a new umbrella or clustered opportunity. Subsequently, the feasibility-impact evaluation of the clustered opportunities was done by voting of the VALKYRIES project partners in which each partner in the consortium had one vote. The results of the voting for each clustered opportunity, both its feasibility and its impact, resulted in prioritisation of 17 harmonisation opportunities with the highest overall feasibility-impact score.

The final stage of the VALKYRIES project execution is creation of harmonization roadmaps of some of the discovered technological, procedural and collaborative and training opportunities for enhancing the Pan-European preparedness and cross-sectorial collaboration for first aid response on multi-casualty disasters.

The prioritized harmonization opportunities have been demonstrated and tested in four cross-border cross-sectorial Use Cases (UCs).

The scenario of the first UC focuses on a large-scale forest fire on the border between Spain and Portugal.

The second UC is about an industrial accident in a factory with tons of flammable materials causing a fire and spills of toxic lead on the border between Slovakia and Austria.

The third UC scenario includes a strong earthquake on the border between Bulgaria and Greece, heavy flood and chemical pollution of the water in the Struma River.

Finally, the scenario of the fourth UC is about a maritime accident among a tanker

ship and a passenger ship in the international waters between Norway, the Netherlands and Denmark with large oil spill.
The common ground of all scenarios is that they are cross-border (affecting at least two countries; Besides, they are related to a MCI; Finally, they require cross-sectorial and cross-border cooperation to manage effectively the crisis situation.
During these UCs several technological solutions in support of the work of the first responders to improve situational awareness, obtaining common operational picture and digitalization of triage have been demonstrated and tested. Besides, during the UCs execution will be tested approaches for harmonization of emergency response plans and operative procedures; Last but not least, in the course of the UCs execution a Joint multinational and interdisciplinary training curriculum will be presented to different groups of first responders who need to acquire basic knowledge and practical skills for performing life-saving activities in various types of trauma and medical conditions in case of cross-border MCI, including using advanced tech technological tools for triage.

Acknowledgements
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.101020676. 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.

ANCHISE

ART-CH: An Advanced Reasoning Tool for Fighting Trafficking of Cultural Heritage

Theodoros Alexakis[1*], Nikolaos Peppes[1], Evgenia Adamopoulou[1] and Konstantinos Demestichas[2]

1. Institute of Communication and Computer Systems, School of Electrical and Computer Engineering, National Technical University of Athens
2. Department of Agricultural Economics and Rural Development, Agricultural University of Athens

Abstract: Looting and illicit trafficking of cultural objects pose a significant threat to the preservation of cultural heritage. Advanced digital tools for the early detection of such phenomena can play an important role in safeguarding the cultural property on a global scale. Towards this direction, this paper demonstrates the main functionalities provided by an Advanced Reasoning Tool (ART) for fighting trafficking of Cultural Heritage (CH) called ART-CH. ART-CH will apply logical, rule-based reasoning which can reveal new relations between the source and the destination points of stolen objects, between the different types of goods and their distribution channels as well as between different structures and activities of traffickers. ART-CH will be based on the W3C Web Ontology Language-OWL and will be tailored to the specific needs of authorities dealing with the illicit trading of antiquities and archaeologists.

1. Introduction

Looting and trafficking of cultural property is a serious problem undermining the cultural heritage on a global scale. The revenues from such illicit activities are extremely high and are estimated to be of billions of dollars annually. These phenomena are very usual in countries facing crises and conflicts, while the money from such activities is also used to support terrorist activities in many cases [1]. Robbery and trafficking of cultural property is often characterized by traits found in organized crime [2]. Illicit online sales on the dark web using cryptocurrencies, the utilization of false documentation and person to person trade are some examples of how the aforementioned activities take place [3].

ART-CH which is presented herein will apply rule-based reasoning and will reveal hidden relations relevant to the activities of looters/traffickers. Such relations can be found in the source and destination points of cultural artefacts, in the traits and activities of illicit traders, in the distribution channels of cultural property, in illicit online listings referring to artefacts, etc. Thus, the envisioned tool will play an active role in the fight of LEAs against trafficking of cultural heritage. The next section describes in more detail the architecture and functionalities of the ART-CH tool.

2. Proposed solution

ART-CH will be based on the SWRL language [4], will apply rule-based reasoning in existing data, and will be able to infer logical conclusions from stated facts as well as to evaluate if these conclusions are complete/consistent. In addition to this, ART-CH will use predefined rules to determine potential relations among different events or entities which are present in a given database. ART-CH can drastically increase the investigation and anticipation capabilities of LEAs regarding the illicit trading of cultural property, underpinning activities for identifying the traffickers' modus operandi, the source and destination places of looted or stolen artefacts, the distribution channels of traffickers, illicit marketplaces, flows of cultural property, etc.
The integration of SPARQL [5] queries will enable the user to define the rules that will be implemented, These logical rules, will be further analyzed by practioners, in order to ensure that they are suitable for the analysis of a given data input format. Soon after that, the tool will infer useful results for the end-user. It should be noted that both logical as well as probabilistic rules can be integrated in ART-CH.
Figure 1 presents a high-level architecture of ART-CH.

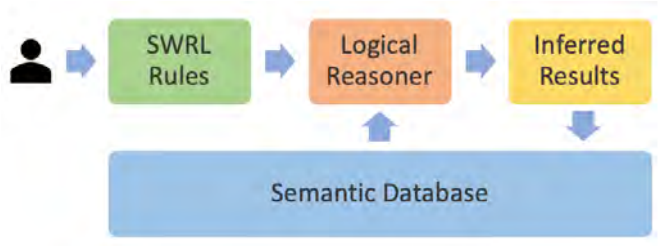


Figure 1. *High-level architecture of the ART-CH tool*

As a first step the expert defines the SWRL logical and probabilistic rules. The Logical Reasoner applies these rules on the data from the semantic database and infers results. The inferred results are then stored to the semantic database.

3. Conclusions and Future Work

The current paper presented ART-CH, a tool that will be developed for fighting trafficking of cultural property. ART-CH will apply rule-based reasoning and reveal previously unknown relations between the source and destination points of stolen artefacts, among diverse distribution channels, among different activities of traffickers, etc. The tool will be based on the SWRL language and future developments will encompass the inclusion of more static rules tailored to the end users' needs as well as the generation of alerts and their publication via a kafka topic.

Acknowledgements

The work described in this paper is performed in the Horizon Europe project ANCHISE ("Applying New solutions for Cultural Heritage protection by Innovative, Scientific, social and economic Engagement"). This project has received funding from the European Union's Horizon Europe research and innovation program under grant agreement No 101094824.

References

1. International Cooperation in Combating Illicit Trafficking in Cultural Property - ProQuest Available online: https://www.proquest.com/docview/2245649480?pq-origsite=gscholar&fromopenview=true (accessed on 24 April 2023).
2. Dietzler, J. On 'Organized Crime' in the Illicit Antiquities Trade: Moving beyond the Definitional Debate. Trends Organ Crim 2013, 16, 329–342, doi:10.1007/s12117-012-9182-0.
3. Paul, K.A. Ancient Artifacts vs. Digital Artifacts: New Tools for Unmasking the Sale of Illicit Antiquities on the Dark Web. Arts 2018, 7, 12, doi:10.3390/arts7020012.
4. SWRL: A Semantic Web Rule Language Combining OWL and RuleML Available online: https://www.w3.org/Submission/SWRL/ (accessed on 26 April 2023).
5. SPARQL 1.1 Overview Available online: https://www.w3.org/TR/sparql11-overview/ (accessed on 25 April 2023).

CTD-TRAC: A Complex Threat Detection Tool for Detecting Illicit Trafficking of Cultural Artefacts

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

1. School of Electrical and Computer Engineering, National Technical University of Athens
2. Department of Agricultural Economy and Development, Agricultural University of Athens

Abstract: The timely recovery of stolen or illicitly trafficked cultural property is of vital importance, as loss of time favors smugglers and can seriously undermine the efforts of protecting cultural heritage. This paper presents a Complex Threat Detection (CTD) tool called CTD-TRAC which will help in the timely detection of illicit trafficking of cultural property. CTD-TRAC will display a wide range of alerts and will be able to provide a unified graph which will help authorities dealing with the illicit trading of antiquities to detect suspicious trafficking activities. The alerts will be generated and broadcasted to the authorities via the respective channels, thus helping to detect smugglers and traffickers before they can proceed to illicit trading. The main architecture, user interface and components featured in CTD-TRAC, will be demonstrated together with the main alerts which will be generated by the tool.

1. Introduction

The prevention of looting and illicit trafficking of cultural objects is of paramount importance for the protection and preservation of the global cultural heritage. Fighting such phenomena requires cooperation among different actors as well as a clear understanding of how illicit antiquities and trafficking networks work [1]. Any loss of time is in favor of the looters/traffickers and can seriously undermine the global cultural heritage. The demand for illicit antiquities often comes from economically and politically secure states which pay looters and sellers from less politically/economi-

cally secure states. There is a quite complex social political and economic structure of the antiquities market which formulates the way different actors are involved in illicit trades [2]. Artificial Intelligence (AI) and advanced Machine Learning (ML) techniques and tools can increase the research capabilities of Law Enforcement Agencies (LEAs) and drastically reduce the time required for combatting trafficking cases [3].

This paper describes the functionalities of the, under development, CTD-TRAC tool. This tool will create unified graphs which can help LEAs, archaeologists or other practitioners and end-users to timely detect suspicious activities related to the illicit trading of antiquities and cultural property. Details about this tool and its architecture, together with screenshots from its User Interface (UI) will be provided herein.

2. Proposed solution

CTD-TRAC is a threat detection tool, which will generate diverse unified graphs related to illicit cultural heritage trading activities. Through this kind of visualization, end users will be able to easily identify correlations between different entities/activities and detect suspicious illegal trading activities and the suspects for these activities. In addition to this, the tool will generate and display alerts as well as broadcast them via kafka topics. Through these alerts, LEAs can timely detect a traffickers/looters and stop them before they laterally move.

More specifically, the types of inputs which can be used by the tool include but are not limited to databases related to illicit trading of antiquities, illicit listings of cultural property in sites or the social media, coordinates of places where illicit activities frequently take place (e.g., near the borders of countries), data from suspicious financial transactions, travel data of suspects of illegal cultural heritage trading, etc. The tool can also be connected to other tools (e.g., make use of the inferred results based on the static rules of a semantic reasoner or make use of the data deriving from a data fusion tool tailored to the needs of cultural trafficking detection).

For creating the unified graphs, CTD-TRAC will use predefined weights based on the existing connections between entities/activities and the number of existing alerts. The exact values of the weights will be defined based on the domain experts' knowledge.

CTD_TRAC will offer an innovative way of identifying diverse types of suspicious/illegal trading activities which undermine the global cultural heritage. The incidents will be detected in real-time or in near-real-time. The above can potentially increase the investigation capabilities of LEAs under the execution of advanced Machine Learning (ML) algorithms, responsible for identifying structured relationships among the different types of entities/activities involved.

Figure 1 contains an indicative screenshot from the User Interface (UI) of CTD-TRAC. In this figure, the connections among different entities are visible, together with some controls integrated which will be available to the user in order to customize the visualization results. It should be noted that the UI may be modified according to the feedback received by end-users.

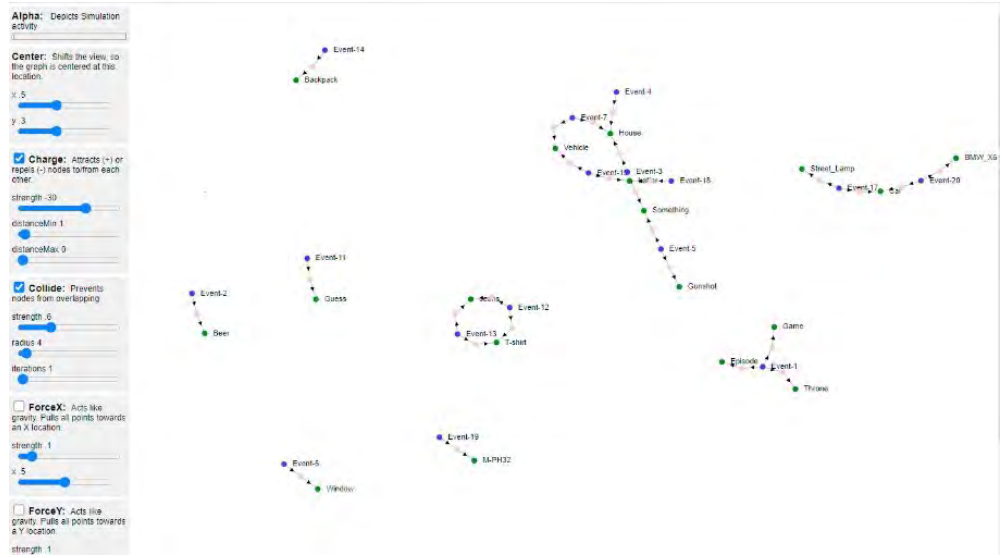


Figure 1. *CTD-TRAC User Interface*

3. Conclusions and Future Work

This paper demonstrates the main functionalities of the CTD-TRAC tool. This tool can help LEAs in the detection of looting and trafficking of cultural artefacts. Based on data retrieved from heterogeneous sources, CTD-TRAC will create unified graphs illustrating potential illicit trading cases and connections among different entities/activities. It will also generate alerts for suspicious trafficking activities of cultural property. These alerts will be provided in real-time and/or in near-real-time to LEAs in order to stop illicit trading before it is completed. CTD-TRAC is currently under development and future steps include the integration of more input sources, the generation of more types of real-time alerts, and the completion of an API of the tool.

Acknowledgements
The work described in this paper is performed in the Horizon Europe project ANCHISE ("Applying New solutions for Cultural Heritage protection by Innovative, Scientific, social and economic Engagement"). This project has received funding from the European Union's Horizon Europe research and innovation program under grant agreement No 101094824.

References
1. Zeynep, B. Fighting the Illicit Trafficking of Cultural Property: A Toolkit for European Judiciary and Law Enforcement; UNESCO Publishing, 2018; ISBN 978-92-3-100289-2.
2. Mackenzie, S.; Brodie, N.; Yates, D.; Tsirogiannis, C. Trafficking Culture: New Directions in Researching the Global Market in Illicit Antiquities; Routledge, 2019; ISBN 978-1-315-53219-6.
3. Abate, D.; Paolanti, M.; Pierdicca, R.; Link to external site, this link will open in a new window; Lampropoulos, A.; Toumbas, K.; Agapiou, A.; Vergis, S.; Malinverni, E.; Petrides, K.; et al. Significance. Stop Illicit Heritage Trafficking with Artificial Intelligence. In Proceedings of the The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences; Copernicus GmbH: Gottingen, Germany, 2022; Vol. XLIII-B2-2022, pp. 729–736.

CESAGRAM

Towards the Prevention and Detection of Grooming Content Online, through AI-based technologies, Training and Awareness Raising Activities: The CESAGRAM solution

Alexandros Koufakis[1], Theoni Spathi[1], Nikolaos Stylianou[1], Georgios Kalpakis[1], Stefanos Alevizos[2], Annika Drandaki[2], Serena Bressan[3], Annapaola Marconi[3], Katerina Georgakopoulou[4], Freideriki Makri[4], Christianna Aposkiti[4], Agathi Barbaki[4], Marva Arabatzi[4], Ruta Grigaliunaite[5], Sarah Brown[6], Rushelle Reid[6], Rhiannon-Faye McDonald[6], Georgia Pasa[7], Naoum Mengoudis[7], Tsakalou Chrysoula[7], Athena Agorgianitou[8], Arūnė Bernatonytė[9], Natalja Kurčinskaja[9], Charlotte Somers[10], Jennifer Schatz[11], Aagje Ieven[11], Theodora Tsikrika[1], Stefanos Vrochidis[1]

1. Information Technologies Institute, Center for Research and Technology Hellas
2. The Smile of the Child
3. Fondazione Bruno Kessler
4. Center for Security Studies (KEMEA)
5. CESIE
6. Marie Collins Foundation
7. Hellenic Police
8. Ministry of Justice, Transparency and Human Rights
9. Missing Persons' Families Support Center
10. Katholieke Universiteit Leuven
11. European Federation for Missing and Sexually Exploited Children

1. Introduction: Setting the Scene
Fastest growing crimes in the recent years, with reporting of suspected online sexual abuse material having outstandingly increased by 35% to 29.3 million reports, compared to 2020 (Negreiro, 2022). The proliferation of online Social Networking Communities as depicted in the growing numbers of social media users - more than 4.76 billion social media users worldwide accounting for 59,4% of the global population with 75% of internet users to be young people among 15-24 years old

(Petrosyan, 2023)- has intensified the growing phenomenon of CSA and especially online grooming activities. COVID-19 crisis has also added to the proliferation of such phenomena, fact underlined in Europol's Internet Organised Crime Threat Assessment (2021). According to the latest report of Internet Watch Foundation (2022) out of the 375,230 reports that have been assessed, one out of five belonged to children aged 7-10 who had been groomed by online perpetrators. Worldwide, more than 60% of online CSAM is hosted in servers based in European Union (EU) (European Union, 2022). Anecdotal information from the 116000 hotlines of Missing Children Europe, has revealed a worrying link between grooming online activities and missing children's cases underlining the importance of further research for effective responses against such phenomena.

2. CESAGRAM response

CESAGRAM (Towards a Comprehensive European Strategy Against tech-facilitated GRooming And Missing) is a two-year European Funded project 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 CSA and missing-children cases, a sector currently under-researched. Since the early stages of the project, innovative desk and empirical (semi-structured interviews, case-file analysis) research that focuses on the connections between grooming for sexual purposes and missing children as well as the applicable legal framework, will aim to outline a comprehensive approach to the phenomenon. It will provide well-rounded knowledge about risk factors for tech facilitated grooming (connected also to missing cases), giving a better understanding of victims' experiences as well as of the criteria for victims' identification. Through adopting a human-centered approach on the identification of user gaps, needs and requirements CESAGRAM will develop certain training and awareness raising tools, targeted to frontline professionals (social workers, NGOs, law enforcement) and policy makers. Furthermore, preventive campaigns targeting children and their carers will also be delivered through an online gamified educational platform developed during the lifespan of the project. A set of AI tools that will facilitate the prevention and detection of grooming content online, facilitating the work of law enforcement, is also one of the cornerstones of this project. Continuous monitoring of online spaces for grooming related content through appropriately configured tools, application of different types of linguistic analysis to the gathered textual material for the detection of grooming activities and their categorization into taxonomies relevant to grooming behaviors will result to the development of AI-based risk assessment for decision support and early warning generation. Finally, through the establishment of the CESAGRAM knowledge hub professionals and experts will build on existing expertise and further promote the project results, raise awareness on CSA, encouraging collaborative and cross-sectoral cooperation on the issue of grooming and missing through networking activities. Policy recommendations for EU policy makers will be produced, along with advocacy training for the effective implementation of EU policies and laws.

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. (2022). Faxctsheet CSA: Fighting child sexual abuse: Commission proposes new rules to protect children. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/fs_22_2978
2. Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021. Luxembourg.: Publications Office of the European Union.
3. Internet Watch Foundation. (2022). The Annual Report 2022 - IWF. Retrieved from https://annualreport2022.iwf.org.uk/wp-content/uploads/2023/04/IWF-Annual-Report-2022_FINAL.pdf
4. Negreiro, M. (2022, December). Retrieved from European Parliament: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf
5. Petrosyan, A. (2023, April 3). Worldwide digital population 2023. Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/

COBRA

COBRA project

Dimitrios Myttas[1], Panagiota Benekou[1], Stavros Magalios[1], Dimitrios Theodosakis[1], Mirela Rosgova[1], Artemisia Nikolaidou[1], Ioannis Galatas[1]

1. KEMEA (Center for Security Studies)

The COBRA Project statutorily aimed to enhance the level of preparedness and response capabilities of southeastern European Law Enforcement Agencies (LEAs) against terrorist attacks to public spaces and CBRN (Chemical, biological, radiological & nuclear defense) threats.
Serving this goal, COBRA invested to the procurement and upgrade of field technical equipment and components, developed training programs and material, and organized field exercises thematically fo-cused to protect and securely respond to terrorist and CBRN threats against CI.
Moreover, COBRA project disseminated and shared project results in context of specialized and sectorial workshops to local, national and EU practitioners involved in the aforementioned type of incidents (e.g., police officers, coast guards, private security personnel, fire-fighters etc.).
In particular, in total four (4) field exercises took place, one (1) in Bulgaria and Cyprus and two (2) in Greece, focused on terrorist attack and CBRN threat, each accompanied by a workshop (Fig. 1).

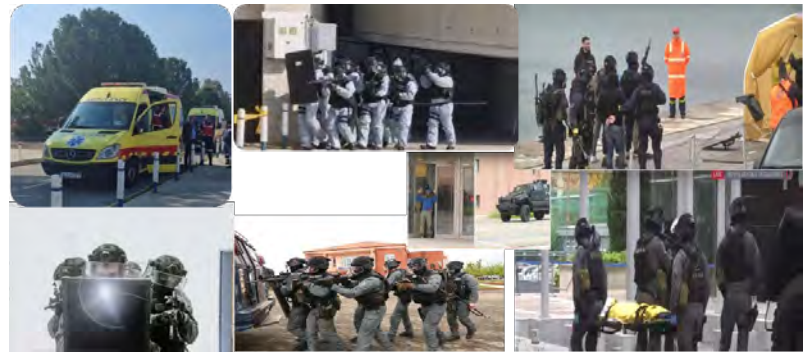


Figure 1: *Field Exercises*

COBRA project results:

• Raised awareness & increased preparedness and response capabilities of south-eastern European Law Enforcement Agencies (LEAs) against CBRN threats and terrorist attacks.
• Developed Training Programs and Material related to CBRN Attacks on soft targets and Terrorist Attacks to CIP.
• Procured CBRN and counterterrorism equipment technology & tools for training and operational purposes.
• Developed a training platform and material for first practitioners.
• Achieving in imparting good practices & lessons learned among 1st-line practitioners involved in COBRA project, in order to facilitate the uniformity of Standard Operational Procedures (SOPs) partaking to the handling of foreseeable cross-jurisdiction incidents.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 861789. 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.

COURAGEOUS

Standardized scenarios and test methods for assessing the performance of Counter-UAS solutions

P. Petsioti[1], G. De Cubber[2], R. Roman[3], A.A. Mohamoud[4], I. Maza[5] and C. Church[6], and A. Koniaris[1]

1. Center Security Studies
2. Royal Military Academy
3. Protection and Guard Service
4. Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
5. GRVC Robotics Lab
6. The International Criminal Police Organization (INTERPOL)

Over the last decades, Unmanned Aircraft Systems (UAS) have been present in a variety of shapes and sizes, ranging from handheld micro-UAS to medium-sized tactical systems to fully grown and Remotely Piloted Aircraft (RPA). At the same time, drones continue to make headlines for their ability to engage in all manner of recreational, but also practical uses, such as search and rescue, surveillance, traffic monitoring, weather monitoring, inspection of infrastructures, firefighting, drone-based photography, videography, agriculture, even delivery services, to name a few. Unfortunately, terrorists and criminals are proving as innovative as their industry counterparts in finding novel uses for UAS. The increasingly common use of drones by terrorists to launch strikes abroad has raised concerns that domestic malefactors may plan and execute similar attacks. Some criminal actors, meanwhile, are using drones to smuggle drugs across the border or into prisons, or otherwise to support their nefarious enterprises. These incidents, as well as others (which include unauthorized flights over sports stadiums or in controlled airspace near airports) have exposed both the vulnerability of sensitive facilities and critical infrastructures to hostile or recklessly operated UAS, as well serious shortcomings in the capabilities of law enforcement and national security agencies to address these threats. The necessity to protect people, infrastructure, and assets signifies the importance of Counter-UAS (C-UAS) systems, including DTI (Detection, Tracking and Identification) systems. In order to be able to evaluate DTI systems, there is a need to develop a set of appropriate standardized scenarios to encapsulate as best as possible the elements involved in the countering of malevolent actions launched by Unmanned Aircraft Systems (UAS).

PROPOSED SOLUTION TOWARDS STANDARDISED TEST DEVELOPMENT

Standard scenario development

The conceptualization of standard UAS threat scenarios is a primary condition required for achieving a common understanding of the capabilities of C-UAS systems. Therefore, the COURAGEOUS project, funded by the European Union's Internal Security Fund Police, develops a set of standard scenarios, representing the needs of all relevant stakeholders and, where possible, find common scenarios. These standard scenarios cover the drone-threat spectrum to the maximum possible extent, against different types of infrastructures, environments, open spaces, etc., under different situations, covering the needs of different stakeholders across European Union Member States.

Under the scope of the COURAGEOUS project, four specific steps were used for gathering and analyzing data related to the development of the standard scenarios, namely:

- Need for standardization Scenarios/Literature review
- Previous incidents & identification of gaps/open data review
- Current C-UAS framework (analysis of different methods & technologies)
- End-User Questionnaire surveys

Performance requirements

In order to find a common agreement on the performance requirements of DTI systems, COURAGEOUS investigates the operational needs of the end users and the corresponding development of functional and interoperability requirements. From that knowledge, COURAGEOUS develops performance indicators for DTI systems, including an evaluation framework aiming to provide a structured tool by which to systematically document, review, compare and evaluate test results for known technology modalities.

Test methodology development

A common understanding of the effectiveness of C-UAS tools can only be achieved when a common, standardized test methodology is adopted to compare different solutions to each other, creating a common understanding baseline. Therefore, COURAGEOUS develops a test environment that is subjected to functional and integral testing in order to serve as a baseline for the qualitative & quantitative evaluation of C-UAS systems. A major constraint is that the methodology should enable testing of different and complete DTI systems under realistic conditions and scenarios. The methodology also covers testing of DTI functions and sub-functions. The methodology is both future proof and able to accommodate future developments.

Performance testing

In order to validate the developed methodologies, and in order to allow for an iterative design review, COURAGEOUS organizes 3 field validation campaigns, geographically spread over the EU, to ensure maximum attendance by industry. The overall aim of this performance testing is to show that the evaluation methodology developed within COURAGEOUS produces quantifiable, documentable, and evaluable performance data on systems under test and also produces comparable evaluation results. In addition, the evaluation results from each test constitute actionable information for stakeholders in the sense that they show how well the specific systems under test address the user needs.

Results dissemination and Standardization

Responsible sharing of research findings is a key element of the COURAGEOUS project, which is a delicate exercise. COURAGEOUS fosters the standardization of its developed test methodology through bodies as EUROCAE, ETSI & CENELEC.

Acknowledgments

The research described in this paper has received funding from the European Union's Internal Security Fund Police under Grant Agreement 101034655 (COURAGEOUS).

CTC

Countering Terrorist Financing with AI Technologies - CTC project

Efstathios Skarlatos[1], Maria Jofre[2], Dimitris Kavallieros[3], Theoni Spathi[3], Theodora Tsikrika[3], Stefanos Vrochidis[3]

1. Center for Security Studies (KEMEA)
2. Crime&Tech - Università Cattolica del Sacro Cuore
3. Centre for Research and Technology Hellas (CERTH)

1. Introduction

Terrorist financing (TF) poses a significant threat to the security and stability of the European Union (EU) and its member states. To combat TF in an efficient and timely manner, advanced technologies must be used (1). The EU-funded "Cut the Cord (CTC)" project seeks to strengthen the EU's capability to better understand and counter TF by exploring the use of innovative technologies and developing AI-based technical solutions.

2. CTC Objectives and methodology

The CTC project aims to (i) advance the understanding of TF methods and trends through cutting-edge research, (ii) enhance and support the public-private partnerships (PPP) through the development and integration of innovative AI-based tools for analysis and detection of TF activities, (iii) create customized training for to advance the expertise of relevant stakeholders and (iv) establish a collaborative platform for sharing data and intelligence. CTC capitalizes on an end-user driven, 4-phase methodology having as its main objective to portray the user's operational, procedural and organizational needs, integrating the final outcomes to the training and technical solutions developed, thus facilitating cross-border and cross-agency collaboration.

3. Desk research

To identify relevant threats and trends in the modus operandi of the TF networks, a comprehensive assessment was performed based on the review of relevant sources (e.g., public and private sector intelligence, police and judicial reports, EU legislation, academic literature, media articles etc.), with special consideration to the FinTech industry (e.g., cryptocurrencies, online payment systems) and other emerging technologies (e.g., social media). Results of the assessment suggest three main categories of TF threats and trends (2): (i) associated with more traditional systems and techniques (cash smuggling, Hawala, bank accounts, money transfer services, false trade invoicing, high-value commodities, internet-based payment systems and e-commerce); (ii) related to emerging payment systems and obfuscation techniques (e.g. cryptocurrencies, crowdfunding, mixers, chain-hopping, shared digital wallets and Metaverse), and (iii) associated with Internet-based communication platforms and social media, which are also related to terrorist purposes other than fundraising, including recruiting new members, spreading propaganda messages and disseminating technical knowledge.

4. Technical solutions

The project proposes a combination of tools to address the challenges posed by TF. These tools aim to track and analyze transactions involving cryptocurrencies as well as traditional financial systems, to further detect suspicious transactions and anomalous patterns, providing in parallel actionable insights to counteractions. They will automatically acquire, process, and store data from various open sources (social media, forums, websites), analyze large volumes of textual content in multiple languages identifying keywords and semantic relationships relevant to TF, and detect clusters, communities and influencers involved in or promoting TF activities, providing valuable insight into the connections and relationships between individuals and organizations.

Advanced machine learning techniques will be employed to identify patterns, trends, and anomalies in large datasets, while data correlation from different sources and modalities will provide a more comprehensive understanding of TF activities and actors. A blockchain-based infrastructure will securely manage digital identities, enhancing trust and collaboration between stakeholders and end-users, while a suite of secure data sharing services will facilitate collaboration and information exchange between public and private sectors, fostering a more effective approach to countering TF.

5. Conclusions

The CTC project is a major step forward in the fight against terrorist financing in the European Union. By developing and integrating innovative AI-based tools and fostering public-private partnerships, the project holds the promise of significantly enhancing the EU's ability to understand and counter TF activities. As the project progresses, the impact of these technical solutions on countering TF will be closely monitored and assessed to ensure their effectiveness and relevance to stakeholders and end-users.

Acknowledgements

This project was funded by the European Union's Internal Security Fund — Police under Grant Agreement No. 101036276. 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. FATF (2021), Opportunities and Challenges of New Technologies for AML/CFT, FATF, Paris, France, https://www.fatf-gafi.org/publications/ fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html.

2. Jofre, Maria and Aziani, Alberto and Villa, Edoardo, Terrorist Financing and the Use of Traditional and Emerging Financial Technologies. Available at SSRN: https://ssrn.com/abstract=4223469 or http://dx.doi.org/10.2139/ssrn.4223469

INHERIT

INHERIT

Blue is the new white – INHERIT investigations of physical properties of targeted tetraammine copper complexes

Waller, V.[1], Fjällgren, M.[1], Landström, L[1]., Önnerud, H[1]. van der Heijden, A.[2], van Driel, C.[2]

1. Swedish Defence Research Agency (FOI)
2. Netherlands Organisation for Applied Scientific Research (TNO)

1. Background

INHERIT1 stands for INHibitors, Explosives and pRecursors InvesTigation and is a Horizon 2020-funded project ongoing from 2021 to 2024.

Criminals, including terrorists, constantly seek new ways to develop, deploy, and activate dangerous chemicals such as explosives. How these chemicals are manufactured and combined evolves continuously, making the specialised work of law enforcement agencies and reference laboratories a continuous challenge.

There are typically three main categories of explosives: military, commercial, and homemade explosives (HMEs). Professionals use the two first categories that are developed to fulfil specific criteria such as high performance and low sensitivity to impact and ageing. The last mentioned category has only one use, which is for harming society via terrorist attacks or organised crime. Many precursors can be acquired in the ordinary retail as consumer products and mixed to make HMEs. Recipes on explosive production are readily available via different manuals and on the internet.

The terrorism timeline consists of multiple phases, where all phases possess vulnerabilities that can be used to disrupt an attack. Due to the large diversity in explosives precursors, there is yet no universal approach to keep a terrorist from using them to make explosives.

The EU precursor legislation2 is an example of a disruption of the terrorism timeline. This action restricts the availability of a precursor, either by a ban, a concentration limit, or through requested reporting of suspicious transactions to authorities. Mandating dilution of a precursor, or reporting requirements of its purchase, allows for regular use while disrupting the illicit application. Despite existing precursor restrictions, HMEs can be made from consumer products. INHERIT aims to further prevent explosive production by restricting access to precursors and detecting them at an early stage. Improvised explosive devices based on explosive peroxide compounds have become a preferred choice among terrorist organisations worldwide. INHERIT is working on developing inhibitors (small amounts of admixtures added to precursors) to obstruct the production of such explosives.

In addition, INHERIT aims to intervene across the terrorism timeline by developing methods and technologies that make explosive precursors inert against misuse, easier to detect, and yield greater forensic value (see Figure 1). In order to realize these aims, it is fundamental to understand and follow current and emerging threats linked to HMEs, how they are synthesized, i.e., from which precursors they are produced from. Furthermore, synthesis of emerging HMEs creates opportunities to work on the development of other countermeasures such as detection and analysis of explosives. These are of importance to improve forensic investigations.

The chemical and physical characteristics of the HMEs also need thorough assessments. The availability of chemical and physical data supports the possible interventions in the terrorism timeline at multiple phases, which emphasizes the importance of research activities aiming at gathering the required knowledge.

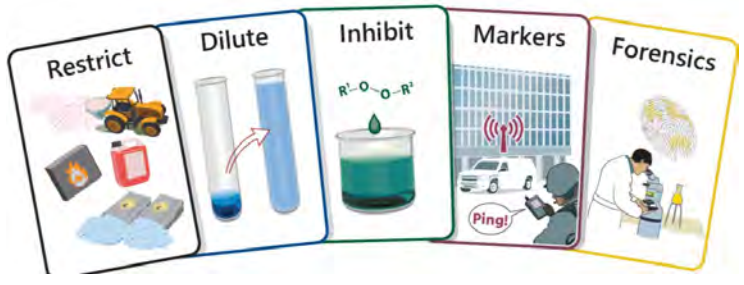


Figure 1. *The foundations of the INHERIT research*

1.1 Explosive tetraammine copper complexes

Most explosives, including HMEs, have a white appearance, however, one group of chemical substances that have been observed to be mentioned online are some of the tetraammine copper complexes (TAC-X) with deep blue colours such as tetraammine copper perchlorate (TACP), tetraammine copper nitrate (TACN) and tetraammine copper chlorate (TACC), see examples in Figure 2. In theory, X could be several anions possessing oxidizing properties. Depending on the oxidizing anion, a product that has a sensitivity similar to TATP and HMTD may be obtained.

TACP is one of the TAC-X complexes that has emerged in actual casework in Sweden. There are several confirmed routes of synthesis of TACP3 and TACN as well as published data on sensitivity of these complexes. However, we have not found any published data on either chemical or physical characteristics of TACC even though recipes are publicly available. Therefore, this study aims to fill this gap of knowledge by collecting sensitivity data regarding impact, friction as well as electrostatic discharge (ESD). Obtaining sensitivity data is of importance for first responders as well as a reference point in phlegmatisation studies. Furthermore, Raman and IR spectra are presented, which could serve as reference for detection of the complexes in casework. Thermal analysis was used to assess the thermal stability of selected TAC-X complexes. Additional characterization techniques, like XRD or LC-MS, have also been performed on the products.

As mentioned, there is a lack of sensitivity data on a collection of TAC-X, relative to well-known explosives as reference (e.g. PETN, RDX and TNT). Since sensitivity testing is operator dependent, recording the sensitivity data of as many TAC-X complexes as possible using the same equipment and operator will offer more reliable (relative) physical data of these complexes. Therefore, this study further aims at providing a collection of sensitivity data of, e.g., TACP, TACC and TACN.

From performance of "field sensitivity testing", it was found that the impact and friction sensitivity of TACN is on the level of that of RDX. The impact sensitivity of TACC is in the region of that of TATP and HMTD, which are explosives commonly used in terrorist attacks in Europe. Therefore, considering the sensitivity as well as the common precursors used for TAC-X complexes, further collection of mutually comparable chemical and physical data is of importance for e.g. first responders in work for safe disposal of such complexes.

Figure 2. *Photos of TACN (left), TACP (middle) and TACC (right).*

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
3. Vodochodský, O., Künzel, M., Matyáš, R., Kučera, J., Pachman, J. Tetraamminecopper Perchlorate (TACP): Explosive Properties. Propellants Explos. Pyrotech. 2021, 46, 280-285.

LAW-GAME

LAW-GAME

LAW-GAME: ELEVATING EXPERIENTIAL TRAINING THROUGH GAMIFICATION TECHNOLOGIES

Katerina Margariti[1], Pantelis Velanas[1], Christos Malliarakis[1], Vassileios Roussakis[2]

1. European University Cyprus
2. Center for Security Studies

1. AN OUTLINE OF LAW-GAME PROJECT

The aim of our project is to train police officers on the procedure, enhancing the transition between the theory and real-life practice through gamification technologies in a safe and controlled virtual environment. Essential tasks during the creation of LAW-GAME serious game are to virtualize and accurately recreate the real world, by realistically simulating and analyzing aspects of a real-world situations.

Figure 1. *LAW-GAME Platform System Architecture.*

LAW-GAME will introduce an attractive approach to the development of core competencies in:
1. Conducting forensic examination.
2. Effective questioning, threatening, cajoling, persuasion, or negotiation.
3. Recognizing and mitigating potential terrorist attacks.
4. Car accident forensic analysis.

The project is divided into various work packages, each tasked with developing specific modules that will be integrated into the final LAW-GAME platform.
The learning methodology developed by the LAW-GAME consortium will be extensively validated by European end-users, in Greece, Lithuania, Romania, Moldavia, and Estonia, but also in an "all user-groups" pilot in a shared VR environment.

1.1 LAW-GAME Mini Games

The project consists of four separate highly immersive and attractive games, which will be designed and implemented to provide to police officers different type of training. The learning methodology will consist of both theoretical and practical training, taking place in immersive virtual environments.
Crime Scene Investigation (CSI) Mini Game: This will involve basic knowledge of the meaning and scope of CSI process. The game will be played through the role of a forensics expert. In this mode, the trainees will be able to do virtual forensic examinations on both real and hypothetical scenarios.
Police Interview Mini Game: In this game, two types of scenarios are performed, the interrogation and negotiation scenarios. The practical courses will utilize immersive virtual reality (VR) environments and human-agent interrogation and negotiation settings. The trainee interview skills will be evaluated based on both the interrogation/negotiation outcome, knowledge and emotional intelligence.
Terrorist Attack Mini Game: The 3rd training module deals with the best police tactics, techniques, and procedures (TTPs) for the prevention of a terrorist attack. Generating in-Game data and applying an analytics framework into the LAW-GAME serious game context will support Law Enforcement Agencies (LEAs) in predicting potential terroristic actions, as part of strategic-level and tactical-level decision making.
Car Accident Analysis Mini Game: Through the fully immersive 3D gamified training system, the trainee will be introduced to a thorough analysis on the scene investigation process, assisted with state-of-the-art artificial intelligence tools.

Acknowledgements
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021714. 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.

ODYSSEUS

ODYSSEUS – Preventing, Countering, and Investigating Terrorist Attacks through Prognostic, Detection, and Forensic Mechanisms for Explosive Precursors

Nikolai Stoianov[1], Borislav Genov[1], Hristo Hristov[1], Sergey Belkinov[1]

1. Bulgarian Defence Institute

1. ODYSSEUS Project in a nutshell

Recent terrorist attacks in the EU have mostly used Improvised Explosive Devices (IEDs) constructed from Home Made Explosives (HMEs), including the attacks in Madrid in 2004, London in 2005, Paris in 2015, Brussels in 2016, and Manchester and Parsons Green in 2017 , as well as more recent failed and disrupted attacks . Explosive precursors, such as fertiliser-based mixtures, continue to be misused for manufacturing HMEs2, , which constitute a significant threat, since they are relatively easy to make, simple to use, and rather effective, as also exemplified by the 2019 attack in Halle (Germany) which demonstrated a lone actor's capability of manufacturing several IEDs.

Despite recent regulatory initiatives by the European Commission culminating in Regulation (EU) 2019/1148 on the marketing and use of explosive precursors that are considered to have contributed in significantly decreasing the cases involving explosive precursors, dangerous substances remain accessible to terrorists, since such illegitimate users are competent in both misusing chemical products and reactants for manufacturing HMEs and also in exploring the use of new explosive precursors, alternative to the ones already known.

This situation is compounded by multiple factors with significant interplay among them. First, the supply chains of chemicals – including substances misused as explosive precursors for manufacturing HMEs – are significantly complex and diverse1, posing important challenges in their traceability and early warning, while the percentage of explosive precursors and other potentially dangerous chemicals purchased online is increasing, making difficult to trace their trajectory. In addi-

tion, access to HME- and IED-making knowledge is for the most part facilitated by readily available open online sources (including social networking sites, websites, and Internet forums)2, often transferring techniques and procedures from conflict zones. Moreover, the prevention of terrorist attacks involving the use of HMEs would substantially benefit from mechanisms enabling the detection of explosive precursors during the HMEs manufacturing stage, whereas after an incident takes place, support for effective and efficient in situ analysis would allow for advanced forensic capabilities. Finally, the level of detection of threats is largely fragmented throughout Europe, exhibiting varying levels of reporting readiness and effectiveness.

The ODYSSEUS Project aims to improve the prognostic intelligence, detection, and forensic capabilities of LEAs and Competent Authorities through developing mechanisms and solutions in order to:

(1) Discover potentially hitherto unknown information about explosive precursors and HMEs based on (i) gathering, mining, and understanding HME-related multilingual and multimedia online content in order to extract knowledge about (possibly unknown) precursors, and (ii) the subsequent characterisation and analysis of selected precursors, including precursors not previously studied, for the determination of their explosive properties, feasibility, and potential for becoming a threat through appropriate theoretical and experimental investigations and tests. This new knowledge will be acquired by building upon HOMER's rich insights on exploiting relevant data mining technologies (such as web crawlers, visual analysis, and multimodal data analytics) to further develop effective and efficient tools for the continuous discovery, identification, retrieval, and analysis of HME-related online content by leveraging the latest advances in Artificial Intelligence (AI) techniques.

(2) Monitor chemical supply chain operations in order to identify anomalous patterns that may predict future threats; to this end regulatory requirements5, and potentially suspicious activities indicators will be leveraged, such as large number of units or quantities requested, vague or illogical stated intended use, non-justified concertation for the intended use, etc. ODYSSEUS will thus enable economic operators and relevant authorities (including LEAs) to satisfy the regulatory requirements regarding the "reporting of suspicious transactions"5 by developing intelligent tools and solutions that will detect irregularities, recognise patterns, and predict trends in transactions associated with the acquisition of potentially harmful substances (such as explosive precursors) across the chemical supply chain ecosystem (with particular focus on chemical marketplaces). To this end, transactional data, coupled with geo-relevant and client behaviour data, will be exploited to improve the prognostic detection, localisation, and assessment of potential threats based on semantically-enhanced methods using blockchain- and AI-based technologies. As a result, supply chain irregularities will be classified according to risk factors and provide an early-warning trigger which could initiate a geo-locating detection mechanism.

(3) Detect potential threats in identified areas of interest, including detection of HMEs at the manufacturing stage. Towards the detection of clandestine labs, ODYSSEUS will design, develop and test novel sensors for monitoring sewerage systems in order to detecting intermediates and impurities associated with the manufacturing process, together with air emissions from targeted areas. In particular, ODYSSEUS will adapt and optimise detectors for (i) gas phase precursor detection and identification by advancing GC-PID (Gas Chromatography - Photo Ionization Detection) methods, and (ii) substance detection in water in (near) real time by combining and advancing state-of-the-art vaporisers, quantum cascade lasers (QCLs), and photo-acoustic detectors.

(4) Facilitate mobile detection of explosive precursors by using Unmanned Autonomous (Aerial and Ground) Vehicles (UAVs/UGVs) equipped with the developed sensors. UAVs will enable air monitoring, while UGVs could be deployed for detecting explosive precursors both at the gas phase and also in sewerage systems in (near) real time; in the latter case, the UGVs will be ruggedised and protected against ingress of dust and water to endure the special conditions. Using such focused and multi-faceted detection mechanisms, together with the outcomes of advanced hydrological-hydraulic and air dispersion models, will allow for the localisation of the sources of the explosive precursors and an assessment of the associated level of threat.

(5) Support forensic investigations through automated sample collection by robotised tools. Robotised tools equipped with appropriate actuators will allow for improving in-situ sample collection; this coupled with the aforementioned mobile detection and threat assessment capabilities will allow to inform the forensic team prior to their physical involvement, thus creating safer conditions for on-site operators and for any civilians in proximity.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021857. 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 in-formation it contains..

References

1. ODYSSEUS Project Grand agreement
2. https://odysseus-h2020.eu/

Participation

PARTICIPATION

Analyzing and Preventing Extremism via Participation

Youssef Bouali[1], Nina Czyżewska[1]

1. Polish Platform for Homeland Security

1. Socio-environmental context and factors leading to violent extremism, radicalization and polarization

In the context of the PARTICIPATION project, one research line aims to broaden the spectrum of understanding of early detection and situation analysis tools regarding the factors that lead to radicalisation, polarisation, alienation and violent extremism. Specifically, work intended to analyze the socio-environmental context in which the factors leading to the above-mentioned processes happen through research in urban and peri-urban areas, especially with regard to the youth population. This latter focus of research and analysis is considered apical by the PARTCIPATION project consortium and research teams as it constitutes one of the largest gaps found in the literature review on radicalization, polarisation, alienation and violent extremism. It should be emphasized that this gap in the literature does not represent a simple academic and cognitive gap, but reflects the delay and, sometimes, obsolescence, both of the risk assessment tools and of the institutional policies to combat and prevent the aforementioned phenomena. Delay and obsolescence that should not be underestimated in order to avoid the risk of being unprepared in dealing with the new forms of violent extremism that are harbouring in European societies and which, to date, can no longer simply be ascribed to the operational perimeter of "terrorism", in that ideological of the extreme right, the extreme left and the religious and social fanaticism of the prison population or the second generations of immigrants.

1.1 Purpose and Methodology

The purpose of this writing is to investigate the perception and existence of radical-

ization, polarisation, alienation and violent extremism factors in local youth communities in an urban and peri-urban area of Poland, Italy and Greece.
The methodology followed for the research and analysis of the data has been properly designed for the PARTICIPATION project, i.e. "Guidelines for Community Mapping activities", which clarified which methodologies to follow to carry out social research and analysis in specific urban and peri-urban areas. The work follows those guidelines and applies them to the concrete case, investigating the opinions, points of view, ideas and fears of the youth population (through a sample coming from high schools) regarding radicalization, polarization, alienation and violent extremism. Students in Polish, Italian and Greek schools participated in Community Mapping activities and "tested" the model of social labs which, in the intentions of the PARTCIPATION project, must help improve the degree of involvement and awareness of local communities, must offer new data and information on the evolutionary path of the factors of radicalization, polarization alienation and violent extremism and, finally, to support the development of new tools and policies for contrasting and prevention. The urban areas selected for the research were Palermo, Poznan and Pireaus, respectively for Italy, Poland and Greece. At the same time, the peri-urban areas were the Union of Municipalities of the Ceramic District, Syców and Delta Municipality, respectively for Italy, Poland and Greece.

Summary of Findings

The research and data analysis activity highlighted how the perception of the factors of radicalization, polarisation, alienation and violent extremism is uniform in urban and peri-urban communities and how an innovative element such as hate speech is considered almost unanimously as an apical vector for all three phenomena.
However, it is important to observe two differences that deserve to be explored in the future. In fact, while in urban communities there is a greater attribution of importance to emotional and psychological factors, in peri-urban communities there is a greater emphasis on economic and working factors. Similarly, while in urban communities young people have shown greater indulgence, respect and trust towards political institutions (both national and local), in peri-urban communities there has been a more direct and sharp criticism of all representations of state power.
In conclusion, the Community Mapping activities show similar opinions by students and local actors and stakeholders on the factors that foster or prevent forms of radicalization, polarization, alienation and violent extremism. These factors are mainly hatred, bullying, political distinctions of the society into good and bad and hate speech.
On this ground, and taking into consideration the limitations of the present research, the PARTICIPATION survey and social lab findings confirm the 3N model of radicalization, while indicate the need for the correlation between radicalization and spatial factors to be further explored. The impact of the physical environment on crime causation has been explored regarding a variety of deviant behaviors, but there are a lot of spatial characteristics that should be further empirically explored as constitutive elements on the manifestation of radical and extreme viewpoints and behaviors.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 962547. This article reflects only the authors' views, while 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. Deliverable D6.3: Guidelines for Community Mapping activities
2. Deliverable D6.4: Report on the ecological context of radicalisation, polarisation and alienation

PERIVALLON

PERIVALLON: Protecting the EuRopean terrItory from organised enVironmentAl crime through inteLLigent threat detectiON tools

E. Villamor[1], T. Tsikrika[2], J. Berggren[3], J. Thompson[4], A. Karakostas[5], F. Benolli[6], E. Skarlatos[7], A. Staniforth[8], D. Borloo[9], V. Efstathiou[10], E. Korenjak[11], N. Haimov[12], M. Radan1[3], D. Bellingeri1[4], R. Bors[15], I. Petropoulos[16], S. Balbierz[17], P. Fraternali[18]

1. ETRA INVESTIGACIÓN Y DESARROLLO, S.A.
2. Information Technologies Institute, CERTH
3. SWEDISH POLICE AUTHORITY – NATIONAL FORENSIC CENTRE
4. CENTRIC, Sheffield Hallam Universit
5. DRAXIS ENVIRONMENTAL SA (DRAXIS)
6. Fondazione SAFE
7. Center for Security Studies (KEMEA), Hellenic Ministry of Citizen Protection
8. Saher (Europe) OÜ
9. R&D Department De Watergroep
10. MarineTraffic
11. Department of Innovation and Digitalisation in Law, University of Vienna
12. Tamar Group LTD., Caesarea
13. SC RadExpert consulting&management SR
14. ARPA Lombardi
15. General Inspectorate of Police
16. Hellenic Police HeadQuarters
17. University of Applied Sciences for Public Services in Bavaria, Department Policing Fürstenfelder
18. Dipartimento di Elettronica Informazione e Bioingegneria, Politecnico di Milano.

Environmental crime and, more specifically, organised environmental crime is identified as one of the key crime threats faced by the EU, being undeniably on the rise. As part of the EMPACT (2022-2025) priorities1 and having a 5-7% yearly growth in number of offenses2, environmental crime has turned into one of the leading crimes on the European and global stage. Intentional dumping of polluting substances, illegal disposal of (hazardous) waste, (cross-border) illegal trafficking of waste, and illegal trade of HFCs are examples of organised environmental crime. Such forms of crime can be challenging to detect and difficult 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.

PERIVALLON is the acronym for the European Commission Horizon Europe co-funded innovation action project entitled: Protecting the European territory from organised environmental crime through intelligent threat detection tools. Its focus is to combat organised environmental crime mainly by: 1) Developing an environmental crime detection and investigation platform at the forefront of technological innovation, and 2) Improving capacity building and international cooperation of security practitioners through enhanced investigation processes. The needs of Police Authorities, Border Guards and Regional and National Authorities will be addressed as the main security practitioners.

To materialise such ambition, PERIVALLON starts with approximately 17 innovative components, most around TRL53: Technology validated in relevant environment. These components will be integrated to build a unique platform providing a single-entry point for the end-users: the PERIVALLON platform. This platform will exploit the latest advancements in Artificial Intelligence (AI) in the fields of geospatial intelligence, remote sensing, online monitoring, and multimodal analytics. The capabilities include: automatic detection of waste disposal and pollutants on land and water based on satellite imagery; optimal inspection and characterisation of sites of interests based on imagery captured by (swarms of) Unmanned Aerial Vehicles (UAVs); optimised X-ray scanning of concealed objects; multimedia-multilingual online monitoring and content analysis; maritime routes prediction; pattern recognition; real-time risk assessment; predictive analysis; audit trail and secure evidence collection and exchange; and holistic situational awareness. Multidimensional integration of multimodal sensor data, ranging from satellite images, video streams from cameras mounted on UAVs, to information gathered from publicly available online sources and related administrative documents, is at the core of the PERIVALLON platform. Through the analysis and correlation of such multimodal information, the platform will support explainable decision-making by all relevant security practitioners towards detecting, investigating, and preventing environmental crimes. Further, international cooperation and secure evidence collection will be established through improved data sharing and blockchain technologies.

Moreover, PERIVALLON provides a comprehensive intelligence picture of environmental crime in Europe through its Environmental Crime Observatory. It identifies types of environmental crime in Europe and its prevalence in the EU countries, outlines their impact on the societal level, analyses the key actors involved and its links to organized crime groups and networks, with particular focus on their modus operandi both online and offline. The insights obtained will be exploited to derive enhanced investigation processes and methodologies. Comparable EU statistics as well as surveys with the relevant security practitioners will provide a multi-perspective foundation of the Observatory.
Moreover, the capacities of the involved security practitioners will be improved through PERIVALLON by means of extensive training, hands-on experience, joint exercises, and testing of key technologies in relevant environments, boosting the uptake of the PERIVALLON technological stack. To this end, the application of PERIVALLON capabilities will be validated in four transnational operational demonstrations, including one EU Agency as well as authorities from Italy, Greece, Belgium, Sweden, Romania, and Moldova.
This paper offers an initial look into the PERIVALLON project, its objectives, ambition, and the technological components that will be integrated into a tailored platform that is expected to significantly increase the capacity of relevant authorities to detect, investigate, and prevent environmental crimes in Europe and beyond.

References:

1. Colantoni, L., & Bianchi, M. (2020). Fighting Environmental Crime in Europe. Preliminary Report.
2. EU Policy Cycle - EMPACT | Europol. (n.d.). Retrieved April 4, 2023, from https://www.europol.europa.eu/crime-areas-and-statistics/empact
3. European Commission. Technology Readiness Levels (TRL). HORIZON 202 - WORK PROGRAMME 2014-2015. Annex G [Internet]. 2014. Available from: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

ProSPeReS

ProSPeReS
Vulnerability Assessment for EU Places of Worship

Konstantinos Apostolou[1], Joseph Levis[1], Christina Karafylli[1], Maria Karafylli[1], Vivian Gravenberch[2], Anna Van der Stok[2], Rafal Batkowski[3], Marcin Podogrocki[3], Timo Hellenberg[4], Hannu Rantannen[4]

1. Center for Security Studies (KEMEA)
2. Dutch Institute for Safe and Secure Spaces (DISSS)
3. University of Lodz
4. Hellenberg International

Extended Abstract

Aimed toward increasing the protection level of Places of Worship (PW) in the EU, the ProSPeReS project follows a risk-based approach, which among other activities, includes Vulnerability Assessments (VAs) for selected PW.
A VA is part of risk assessment (ISO, 2018) and it entails the examination of assets, security measures, policies, and procedures at a site of interest, in order to identify its weaknesses against potential attacks against it. It is a cooperative and multidisciplinary process, acknowledged as a good practice by the European Union (EU) (EC, 2019) for improving the Protection of Public Spaces of the EU Member States, including PW.
VA workshops have been performed by the ProSPeReS consortium (including site surveys), and have been organised for a) the Christian Orthodox Church of Saint Paisios (Ioannina, Greece), b) the Catholic Archcathedral of Stanislaus Kostka (Lodz, Poland) and c) Nozyk Synagogue (Warsaw, Poland). The aim of the workshops was to identify common security needs and gaps and to exchange good practices for the protection of their PW, while bringing together the PW's management and staff, local law enforcement officers and emergency responders in order to get actively involved in the VA process, discuss various threat scenarios and consider solutions,

as well as a joint and coordinated approach for the protection of their sites in preparation of and during large religious events.
The workshop execution approach followed the methodology introduced by the EU Vulnerability Assessment Tool (VAT), later enhanced and renamed to Vulnerability Assessment Checklist (VAC)[4], developed by European Union's Directorate General for Migration and Home Affaires (DG HOME).
Following the workshops, additional case studies of religious sites across the EU were investigated through targeted questionnaires, interviews and site visits in order to identify their common and distinctive challenges, vulnerabilities and needs.
Furthermore, ProSPeReS has developed a summarised version of the VAT, namely "VAT Lite". VAT Lite is intended to assist the operator and staff of a PW to carry out a quick VA, focusing on the PW's daily activities, rather than high profile and large-scale religious events. The VAT lite has been tested through the activities of the project for further improvement and will be presented in more detail.
Identified Vulnerabilities at PW
In general, the identified vulnerabilities at the examined PWs are related not only a lack of technical security measures, but also to risk awareness and the security culture of the religious staff and operator, to emergency response training, and lack of communication and collaboration between the religious staff and local stakeholders responsible for the protection of the sites.

Identified Challenges

Various sociotechnical challenges in respect to the protection of PW will be discussed, related to legal restrictions, acceptance by the community, and the site operators' security and organisational culture shaped by the nature and purpose of the PW and their service to the community.

Recommendations

Traditional security measures such as x-ray machines or video surveillance systems might not always be applicable or effective. As a response, in addition to the technical measures, suggestions based on the identified vulnerabilities will be presented, including novel sociotechnical methods for raising the protection of PW, bringing together law enforcement authorities, emergency responders, religious staff, and the religious communities.

4. Not published at the time of this Abstract.

Acknowledgements

This project has received funding from the European Union's Internal Security Fund — Police under grant agreement No. 101034230. 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. ISO. (2018). Risk management — Guidelines. ISO 31000:2018. Available at: https://www.iso.org/iso-31000-risk-management.html
2. European Commission. (2019). Commission Staff Working Document: Good practices to support the protection of public spaces. Available at: COMMISSION STAFF WORKING DOCUMENT Good practices to support the protection of public spaces Accompanying the document Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union - Publications Office of the EU (europa.eu)

Secu4All

Strengthening local authorities' capabilities and capacities regarding the protection of public space: a co-productive approach

Vivian Gravenberch[1], Sara Houweling[2], Paul van Soomeren[3] and Pilar de la Torre.

1. Dutch Institute for Safe and Secure Spaces (Stichting DISSS)
2. European Forum for Urban Security (Efus)

1. Introduction

This abstract is based on the research carried out as part of the Secu4All project, and the training that was developed as part of this project. The Secu4All project is composed of a consortium of 13 partners, including four local and regional authorities (Brussels Capital Region (Belgium), Riga Municipal Police (Latvia), City of Xábia (Spain), City of The Hague (Netherlands)), as well as five organisations and academic partners (European Organisation for Security-EOS, The Center for Security Studies-KEMEA (Greece), Dutch Institute for Safe and Secure Spaces, DISSS (Netherlands), DSP-groep (Netherlands), CRIMINA centre of the Miguel Hernandez University in Elche (Spain)) and three national Fora (German, French and Italian Forum for Urban Security (DEFUS, FFSU, FISU))[3].

The project was instigated by the need of local and regional actors involved in the security of public spaces for a) more theoretical knowledge and b) more practical tools to contribute to the security of public spaces and the protection of soft targets. The public spaces this research focuses on includes soft targets such as sports venues, shopping centres and schools, as well as other public spaces where citizens gather[1]. These public spaces in cities are dense and rich places of exchange, culture, commerce and leisure. Because they are highly frequented and have an open character, they can be subjected to a number of threats, such as terrorism, crime, natural disaster or crowd gatherings. Ensuring that these public spaces remain open, accessible, inclusive and safe is a complex challenge.

Another reason why the protection of these places is challenging, is due to the fact that local and regional authorities need various stakeholders to cooperate with, when it comes to a successful approach to protecting public spaces. These stakeholders come from various backgrounds, in both the public and private sector, including urban planners, first responders, mobility services, and local business owners. In the current climate (pre-Secu4All), there is a gap between the local and regional authorities, and those who are in the first line when it comes to anticipating, presenting, and mitigating security risks and threats to which public spaces are exposed. Between these parties there is incredible knowledge and experience, however sufficient knowledge exchange and cooperation is lacking.

The Secu4All project aims to empower local and regional authorities with theoretical knowledge and practical tools to ensure the security of public spaces and the protection of soft targets against potential threats. In addition, it strives to offer an approach that invites trainees to actively participate, and even have fun while learning about a successful approach to urban security.

2. Method and approach

Within the Secu4All project, the multiple-helix approach (working together with public bodies, research institutions, private organisations and citizens) is a central topic. The project is aimed at empowering local and regional authorities. This was done by developing both on- and offline training, with the online training preceding the offline training. Both trainings were designed with a strong focus on interaction. Especially during the COVID-19 pandemic, where all trainees were in isolation at home, the project strived to create an open dynamic and offer a fun environment while learning.

After completing the online training, the participants were ready for the in situ training. For the in situ, a mixed group of important stakeholders, accompanied by the trainers, visited a chosen Public Space of Interest (PSOI). For the first training module, participants conducted their very own risk assessment at the PSOI, based on the ISO Risk Management Guidelines 31000:2018[2] of the PSOI, and learned how to organise a risk assessment themselves in the future. In the second module, effective ways of crime prevention through environmental design were topics of discussion. For instance, the new CEN Crime Prevention Through Environmental Design (CPTED) standard of implementing not only the technical aspects of designing out crime, but also the social aspects, were discussed in Module 24. The new standard was also tested during the in situ training in Fano, Xàbia, Hannover, Riga, Paris and the

Hague. During the third module, various technologies that can effectively function as a capable guardian against crime were scouted and evaluated. In addition, these technologies were discussed in terms of societal, ethical and legal implications. In the final stage of the training, learners were guided through a fictive crisis and golden hour, either designed by the learners themselves or created by the Center for Security Studies - KEMEA, including training in crisis communication techniques.

3. Conclusion

The Secu4All project has provided comprehensive and co-productive methods, tools and training that can help to increase the capabilities of local and regional authorities. To assist these authorities with the protection of their public spaces, basic (criminological) principles of the protection of public space were explained during an online training. By using mixed effective methods to increase the interoperability and interaction between different stakeholders, the Secu4All project has not only trained local and regional authorities, but has also shown them and other stakeholders how to build a sustainable, comprehensive and practical method of protecting public space. Lastly, Secu4All allows local authorities to build a network of informed and empowered stakeholders to take on the challenge of secure and welcoming public spaces together, including knowledge on how to keep growing and supporting this valuable network.

Acknowledgements

This project has received funding from the European Union's Internal Security Fund – Police under Grant Agreement nº 952789. 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. PRoTECT (2020). Deliverable 2.1. Manual EU VAT. Retrieved on May 4th, 2023. URL: https://protect-cities.eu/wp-content/uploads/2021/02/PRoTECT_Deliverable-2.1-Manual-EU-VAT_v2.0.pdf
2. The International Organization for Standardization (2018). Risk Management - Guidelines.
3. Retrieved on May 4th, 2023. URL: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
4. Efus, Secu4All (2021). Training local authorities to provide citizens with a safe urban environment by reducing risks in public spaces. Retrieved on May 4th, 2023. URL: https://efus.eu/secu4all-en/
5. The new CEN TS 14383-2:2022 supersedes the old TR. It builds on ideas from risk management (ISO 31000 series), Quality management (ISO 9000 series), CPTED (ISO 22341:2021) and new approaches, new types of crime and UN/EU standards/documents (like the ICCS).

SHIELD

SHIELD project: solutionS to enHance Interfaith protEction of pLaces of worship from terrorist Danger

Alessandro Marani[1]

1. Zanasi & Partners

SHIELD is a project funded by the European Union's Internal Security Fund aimed at protecting places of worship from the risks of terrorist attacks and violent extremism To this purpose, the project is currently gathering EU public and private actors - Christian, Jewish and Muslim organisations, security practitioners, LEAs, municipalities, experts in risk detection and technological partners - in order to identify, for each religion, critical points in places of worship (e.g. holy water fonts, matroneums, musalla) as well as circumstances and rituals (e.g. Sunday mass, Shabbat, Jumu a) that are more subject to the risk of terrorist attacks. In addition, SHIELD is identifying the religious buildings (e.g. schools) that are potentially more vulnerable, as well as the types of terrorist attack (e.g. gunmen raids, bioterrorism, etc.) that would be more likely to be perpetrated.

Such risks and sensitive points - backed by an analysis of past attacks - could be tackled by developing new measures and by suiting already existing technologies (e.g. CCTV, sensors) to the above attacks. In addition, tailored recommendations and guidelines for LEAs and religious leaders will be outlined to favour prevention (e.g. identification of suspicious behaviour) and the implementation of common protocols to mitigate the impact of the attacks (e.g. standard evacuation procedures). SHIELD will also produce and distribute factsheets and leaflets to religious leaders, who will actively spread them and raise awareness on terrorist threat among respective communities. Furthermore, training sessions for practitioners and religious leaders will be organised to prove the practical feasibility of recommendations as well as the effectiveness of new solutions and methodologies, which will be tested and validated in joint simulations. Finally, SHIELD will foresee two workshops, with the aim to share and disseminate the results of the project among relevant stakeholders, including EU policymakers and the general public. The 1st workshop has already been organised at the Great Mosque of Rome in December 2022.

SHIELD is divided in 5 work packages:

Work package 1 (WP1) is a standard administration and management WP.

Work package 2 (WP2) is dedicated to the creation of a risk assessment on terrorist attacks to places of worship and religious buildings, respectively for Christianity, Judaism and Islam. Recent terrorist attacks have been reviewed to gather lessons to be learnt and common trends. Vulnerable spots in buildings and rituals or holidays that attract huge crowds have been identified. These activities gave the foundations for the definition of prevention and mitigation strategies, to be identified in WP3.

One of the first outputs of SHIELD an analysis of the state of the art of terrorist attacks on places of worship from the 21st century until today in order to establish a comprehensive understanding of the phenomenon. In addition, the concept of "terrorist attack" was deeply discussed. Countries and organisations often have their own definition of terrorism, which do not necessarily coincide.

Work package 3 (WP3) aims to identify technologies and procedures that can meet the needs and mitigate the vulnerabilities outlined in WP2, to ensure a thorough security of places of worship from terrorism as regards protection of buildings, prevention of attacks and reaction to the event. A VAC (vulnerability assessment checklist) has been created in order to analyse which are the most vulnerable spots and then the suitable countermeasures are proposed.

Work package 4 (WP4) aims at developing training sessions and simulations to test, validate and evaluate the methodological, technological and procedural solutions identified in WP3. The objective is to enhance awareness on and preparedness for different risks of terrorist attacks to places of worship and religious buildings.

Work package 5 (WP5) is focused on dissemination and communication. One of the objective of WP5 is the creation of a handbook to be distributed to religious communities.

The content of the handbook is still being finalised. Schematically, the content of the handbook will be as follows:

- a brief definition of terrorism and the danger of violent attacks through places of worship caused by their vulnerability;
- a brief focus on the need of awareness of religious communities and in particular of religious leaders and individuals responsible for security;

• a general overview of violent and terrorist attack towards houses of worship in Europe since the 2000's;
• some statistical data about the types of attacks (tactics, weapons used etc) depending on religious building and the vulnerabilities exploited by the attackers;
• some tactical considerations and general vulnerabilities identified and detected in places of worship;
• the presentation of the Vulnerability Assessment Checklist (VAC) adapted for places of worship and the instructions in order to use the instrument;
• a list of the existing solutions in order to develop and increase preparedness towards terrorist attacks like education, creation of a culture of acceptance of a potential danger)
• a list of existing solutions in order to physically protect places of worship like hard security measures but also soft solutions, accessibility of offensive weapons, self-defence capabilities of houses of worships, training of the security personnel but also psychological aspects of possible responses to terrorist attacks.

Acknowledgements
This project has received funding by the European Union's Internal Security Fund under grant agreement N°101034229. 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

SHIELD Project - Water Security Planning for Protection of Places of Worship

Teixeira Rui[1]

1. Municipality of Barreiro

Water is a vital sector that serves communities and businesses on a daily basis. Clean water underpins the essential functions of our society, which makes safeguarding and securing water infrastructure a top priority.
Drinking water systems must be protected against a wide range of threats that can compromise their integrity, quality of service and business continuity. Drinking water distribution networks are particularly vulnerable to intentional threats with little or no prior notice, such as physical acts of sabotage, cyber-attacks, and contamination, which can induce interruption of service and cascade effects, in particular, harm to health of consumers.
Water security planning can help mitigate such risks by ensuring timely detection of events, rapid communication and implementation of resilient measures through the development of a Water Security Plan (WSecP), encompassing key challenges and experiences from the field.
The WSecP design includes a general characterization and a detailed description of the system and all its components, including its redundancies in terms of water supply alternatives. It also incorporates an identification of threats to the system and its vulnerabilities, the constitution of an internal team, and all the external entities that should be part of the plan, allocating roles and responsibilities to all. Finally, the risk assessment culminates in the identification of the most likely risk scenarios for intentional water contamination, cyber-attacks, or weaponized disinformation campaigns. Risk management provides detailed guidance to operators on the creation and implementation of a WSecP in order to reduce and revise periodically the above-mentioned risks to drinking water infrastructure, as an essential part of the WSecP lifecycle. Water security planning consists of four phases, as shown in figure 1.

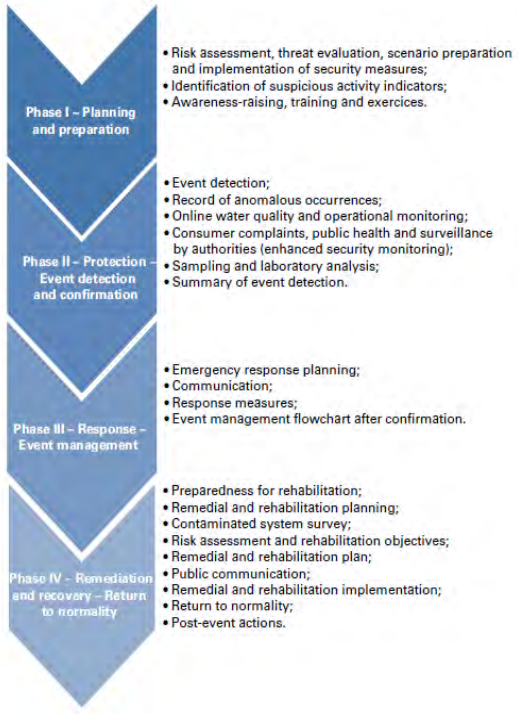


Fig.1. *Phases of a Water Security Plan.*

The Shield Project aims to develop solutions to improve the interfaith protection of places of worship against terrorist danger, and this danger can occur not only by attacks with firearms or explosives, but also by intentional contamination of the drinking water in these places, using certain chemicals that have deadly potential. As such, the Water Security Planning, being in line with the European Counter-Terrorism Strategy and the 2017 EC Action Plan for CBRN risks, is one of the solutions for the protection of those places, through a set of prevention, response and communication measures and plans.

Fig.2. *Objectives of SHIELD Project*

Depicts the lifecycle of a WSecP, from the design of the plan to its implementation, review, and dissemination. The transversal element to all stages is an adequate communication system, fundamental to the success of the process after a malicious event.

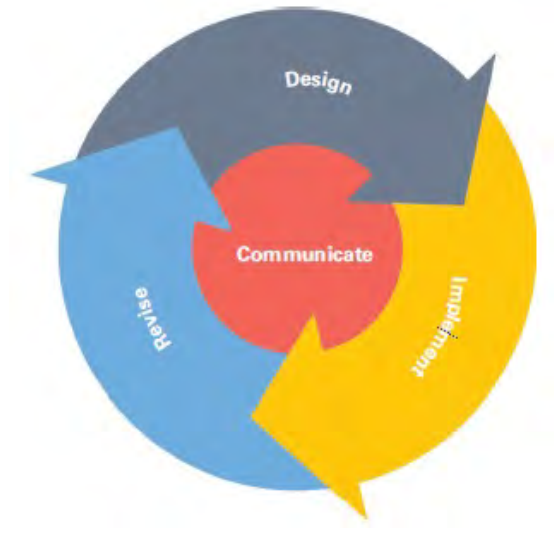


Fig.3. *Water Security Plan Lifecycle.*

The presentation provides a roadmap for water utilities and decision makers to assess security risks to drinking water infrastructure and identifies key elements to consider enhancing detection capabilities in order to respond in a timely manner to hostile actions.

Acknowledgements
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101034229. 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. www.shieldproject.eu
2. TEIXEIRA (R.), CARMI (O.), RAICH (J.), GATTINESI (P.) and HOHENBLUM (P.). – Guidance on the production of a water security plan for drinking water supply (2019).

STARLIGHT

STARLIGHT
Geo-temporal crime forecasting using a Deep Learning attention-based model

Fabio Caffaro[1], Lorenzo Bongiovanni[1], Claudio Rossi[1]

1. LINKS Foundation, AI, Data & Space (ADS)

1. Introduction
Predicting crimes is crucial for law enforcement agencies (LEAs) to help them optimally allocate resources with the scope to better respond to criminal activities [1]. In this sense, it is essential to forecast the possible crime hotspots within narrow regions spatially, as general predictions on larger areas, such as the city or district level, do not allow to design and implement strategies to combat crimes effectively [2]. This paper proposes a deep learning-based approach to address this problem by developing a geo-temporal crime forecasting model that can capture crime incidents' spatial and temporal dependencies.
A substantial amount of previous research has been performed on the application of machine learning for the task of crime predictions [3]. This work addresses one of the future works outlined in previous papers, namely the capability of recent models based on Transformer to enhance the accuracy of crime predictions in an urban setting, targeting a daily temporal resolution and a narrow spatial grid.

2. Data and Method
We utilised the public dataset of Crime Incident Reports from the Boston Police Department.[5]This dataset includes information from August 2015 to December 2022 on crime incidents such as larceny, burglary, and robbery. 468208 crimes are reported in the dataset, with an average of 5202 crimes per month. For each crime, the street, district, date, and crime category are annotated among 34 distinct types. We considered predictions on a grid composed of 1km2 cells. The proposed model

5. https://data.boston.gov/dataset/crime-incident-reports-august-2015-to-date-source-new-system

forecasts the daily number of crimes in each cell with a lead time of 7 days (one week), considering as context the crimes that happened during the previous 30 days on the whole grid. The model takes the array of crime occurrences in each cell during the day as input features. The model is based on an Encoder-Decoder Transformer architecture [4] that consists of multiple layers of self-attention and feedforward networks, which allows the model to capture long-term dependencies in the sequential data.

3. Results

We implemented this work on Google Colaboratory Pro+ with Python 3.10.11, using Pytorch 2.0 for the transformer model (i.e., nn.TransformerEncoder and nn.TransformerDecoder) and scikit-learn for the baseline models (i.e., RandomForestRegressor and LinearRegression). We set the Transformer model with a hidden size equal to 64, a dropout equal to 0.1, and a learning rate of 1e-4, while for the Random Forest model, we use 100 trees and a maximum depth of 4. We evaluated the model's performance by measuring the Mean Average Error (MAE) and Mean Squared Error (MSE) of each cell's predicted daily number of crimes. The dataset was split, considering as a training set all the crimes that happened before the 1st of January 2022 and as a test set all the remaining ones. Our experimental results show that the proposed model outperforms traditional machine learning models, such as the linear regression model [5] and random forest [6] for crime forecasting. As it is possible to observe from Table 1, the Transformer model proposed provides a substantial improvement with respect to standard machine learning models. In particular, the model obtains a score of 1.674 in MSE, achieving a reduction of 68% and about 18% compared to the Linear Regression and Random Forest models, respectively.

Table 1. *The obtained MAE and MSE for different models. The baseline models (Linear Regression and Random Forest) are compared with the proposed Transformer model.*

Model	MAE	MSE
Linear Regression	1.319	5.276
Random Forest	0.797	2.041
Transformer	0.791	1.674

4. Conclusions

Accurate crime predictions can assist law enforcement agencies in allocating resources to effectively address crime in specific areas, thereby improving public safety. In this paper, we proposed a deep learning model based on an Encoder-Decoder Transformer architecture for geo-temporal crime forecasting. The model demonstrated its ability to capture crime incidents' spatial and temporal dependencies and forecast crime patterns, improving the prediction accuracy against baseline models proposed in previous studies. In future work, we plan to extend our model by incorporating additional features (e.g., weather forecasts and land use) to make the model spatially agnostic and scalable to different cities.

Acknowledgements

This project has received EU funding through the STARLIGHT project (grant agreement No. 101021797), the APPRAISE project (grant agreement No. 101021981) and the LAGO project (grant agreement No. 101073951)

References

1. Benbouzid, B. (2019). To predict and to manage. Predictive policing in the United States. Big Data & Society, 6(1).
2. Weisburd, D., Bernasco, W., & Bruinsma, G.J. (2009). Putting crime in its place: Units of analysis in geographic criminology.
3. Jenga, K., Catal, C. & Kar, G. Machine learning in crime prediction. J Ambient Intelligence and Humanized Computing 14, 2887–2913 (2023).
4. Vaswani, Ashish, et al. "Attention is all you need." Advances in neural information processing systems 30 (2017).
5. Nelder, J. A., and R. W. M. Wedderburn. "Generalized Linear Models." Journal of the Royal Statistical Society. Series A (General), vol. 135, no. 3, 1972, pp. 370–84. JSTOR.
6. Breiman, L. Random Forests. Machine Learning 45, 5–32 (2001).

STARLIGHT

Leveraging Continuous Learning for Fighting Misinformation

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

1. Institute of Communication and Computer Systems, School of Electrical and Computer Engineering,
2. Department of Agricultural Economics and Rural Development, Agricultural University of Athens

1. Introduction

The eruption of digitization and the establishment of Social Media as a major content production and reproduction means has led to new paradigms of journalism and news spreading. The rapid changes that took place in the last twenty years led to an environment of pluralism without borders, where, also, may threats are lurking. One of these threats is the rapid spreading of misinformation/disinformation. It is proven that fake news is spreading even to six faster than credible information [1]. This phenomenon consists a major concern firstly for media organizations and professionals as well as for Law Enforcement Agencies (LEAs) due to the fact that the rapid spread of disinformation can severely threaten many aspects of society. According to the European Commission the spread of both disinformation and misinformation can feature a range of harmful consequences, such as the threatening of our democracies, the polarization of debates, and the setting of the health, security and environment of EU citizens at risk [2].

As the practices of misinformation and disinformation evolve it is of utmost importance to design, develop and engage new technologies and solutions in order to tackle such phenomena. In this light, numerous approaches engaging Machine Learning (ML) in order to address this problem from different viewpoints have emerged. Even though, from a technical perspective, several diverse solutions for fake news detection and identification of misinformation, such as transfer learning, multi-task learning, reinforcement learning, online learning etc., do exist, no universal solution to fit in all the aspects of this issue has been developed so far. Almost each and every single solution aims to address the problem in or a very specific topic or domain and based on a limited dataset. The purpose of this study is to present an approach which combines and evaluates the results of different Machine Learning prediction models into a common environment named "Meta-Detection Toolset". This solution relies on the calculation of a meta-score by using weights-based voting among different prediction models, usually referred to as verification services. The weights of the verification services are constantly updated based on the annotation procedure by the end-users of the Toolset. This leverages the current solution into a lifelong learning approach which is future-proof and adaptable as the Machine Learning models improve or aggravate through the course of time or perform better or worse for different topics or styles of writing.

2. Proposed solution

As mentioned, the proposed solution of the Meta-Detection Toolset engages different verification services. These diverse verification services serve as predictors of credibility for a given content source e.g. URL or a text. Based on the integration and implementation of a weighted majority algorithm [3], equal weights are initially assigned to each verification service. During the continuous training process, the weight assigned to a verification service is automatically adjusted according to the accuracy of its predictions. Verification Services with more correct predictions during the training phase, are provided with higher weights, thus playing a more important role when the MDT is calculating the credibility of a certain URL or a text. End-users, e.g. fact-checkers, LEA officers, etc., also play an active role in the training process. More specifically, end-users can insert their credibility evaluation of specific URLs (i.e., indicating whether a specific URL represents legitimate or fake news). The aforementioned users' evaluations are provided in the form of a ground truth label (Legitimate/Fake), are stored in a database, and are utilized during the continuous training phase for updating the weights assigned to each verification service. Thus, a growing number of these annotations will lead to improved verification results of the Meta-Detection Toolset.

The accumulated experience is envisioned to lead to the generation of a model which extensively utilizes contemporary AI technologies for combatting the spread of fake news on the web. This model is comprised of multiple specialized verification services and has the ability to combine verification services based on different methods, aiming to evaluate the truth based on a complex scoring mechanism. This AIbased process is called Meta-Detection and achieves continuous improvement

established by annotation processes performed by specialized end-users.
In the context of the Meta-Detection Toolset, an integrated management environment of the verification services utilized is developed, where the Meta-Detection scores are also determined according to the annotations provided by fact-checkers. More specifically, for a specific URL for example, the annotation of a ground truth label is provided (Legitimate/Fake) by certified fact-checkers. A growing number of these annotations can lead to more accurate verification results in real time. Data ingestion can be achieved either at the end-users' side over the HTTPS protocol or by using data connectors (Kafka topics and/or REST APIs). Then, the input data can be consumed by various verification services integrated in or connected with the toolset. Following the completion of the verification services' computation processes, the prediction results are sent to the MDT and the results are combined in order to compute a meta-score that reflects the credibility of the digital content.

Acknowledgments
The work described in this paper is performed in the H2020 project STARLIGHT ("Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats"). This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 101021797.

References
1. Vosoughi, S.; Roy, D.; Aral, S. The Spread of True and False News Online. Science 2018, 359, 1146–1151, doi:10.1126/science.aap9559.
2. European Commission Tackling Online Disinformation Available online: https://digitalstrategy. ec.europa.eu/en/policies/online-disinformation (accessed on 18 April 2023).
3. Littlestone, N.; Warmuth, M.K. The Weighted Majority Algorithm. Information and Computation 1994, 108, 212–261, doi:https://doi.org/10.1006/inco.1994.1009.

Tools4LEAs

Tools4LEAs
Kriptosare: Behaviour analysis in cryptocurrency transactions

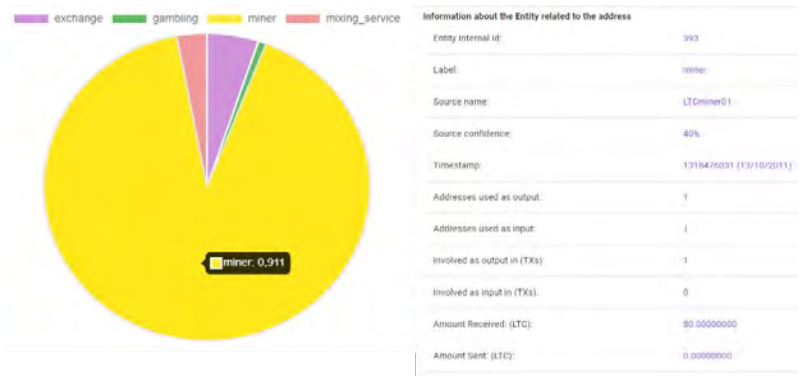
Francesco Zola[1], Jon Elduayen[2], Igor Pallin[1], Raúl Orduna-Urrutia[1]

1. Vicomtech Foundation
2. European Anti-Cybercrime Technology Development Association (EACTDA)

Undoubtedly, the cryptocurrency industry is experiencing rapid innovation and constant evolution, derived from its power and utility. Despite being backed by blockchain technology that promises security, immutability, and full transparency, some cryptocurrencies, Bitcoin imprimis, have been used as enablers for many licit and illicit activities such as trading, buying of goods, money laundering, scam, terrorism financing, ransomware payments, etc. In this scenario, the analysis of the transactions, as well as the entities that have generated them, became a crucial step for Law Enforcement Officer (LEO) investigations. However, the (pseudo) anonymity of the network, the lack of regulatory authority, the employment of anonymizer mechanisms, the evolution of entities' behaviour, and the emergence of new dynamics, are just some of the main elements that make this task challenging. At the same time, the huge amount of information to be analyzed can result in a waste of time and resources, slowing the investigations.
For this reason, in this work, we present Kriptosare, a tool able to classify entity behaviours belonging to three main cryptocurrencies (Bitcoin, Bitcoin Cash, and Litecoin). Kriptosare is composed of a module called Kriptosare.class which makes use of state-of-the-art Machine Learning (ML) techniques to reduce anonymity in the considered cryptocurrencies. This ML model extracts behaviours (or classes) from interactions and dynamics of different known entities involved in the transactions and then predicts the behaviours of new unseen entities. Pre-defined ML models are provided for a first classification, although users can train new ones, and so they can re-classify the whole blockchains. For this task, the blockchain information

is combined with open-source external data containing information about crypto addresses and real-world entity names detected over the years. This additional information facilitates the behaviour definition following the taxonomy provided by Interpol (Exchange, Mixer, Miner Pool, Marketplace, etc.) and represents a ground-truth for the ML training. However, these external data show uneven distribution, i.e., several entity behaviours are more represented than others introducing a class imbalance problem. The imbalance problem is very critical since it can strongly affect ML performance, leading the model to learn skewed scenarios. Furthermore, addressing it is even more challenging in cryptocurrency applications where it is complex and resource and costs expensive to detect and collect new observations data. Indeed, it is easier to find labelled behaviours of entities related to licit transactions rather than the ones involved in illicit activities, which of course, are the most interesting from an investigation point of view.

For this reason, Kriptosare also includes a synthetic data generator module called Kriptosare.gen. This module is a crypto simulator able to create and manage a private Bitcoin, Bitcoin Cash, or Litecoin network. The control of this crypto environment allows users to replicate real behaviours generating synthetic data and then use them to address the imbalance problem introduced by external sources. More specifically, for creating their private network, users have two options, a) deploy normal wallets, i.e., traditional and behavioural-free entities, or b) pre-defined behavioural entities, i.e., intelligent wallets able to replicate real specific behaviour assigned. In this way, on the one hand, it is possible to enhance the performance of the Kritposare.class reducing the costs. On the other hand, LEOs can study behaviours in captivity, i.e., in an isolated and controlled environment, to improve their knowledge about them.



In summary, Kriptosare allows users to manage both the classification and the generator modules in an easy way, through an intuitive and user-friendly interface. To the best of our knowledge, the presented tool can be used by LEOs to search and highlight the most important red flag indicators that could suggest criminal behaviour, for example, a divergence between real labels obtained from external sources and the Kriptosare.class predictions, or the usage of specific entities that are usually involved in illicit activities, such as anonymizer or tumblers. These results can also be used for supporting LEOs' analysis and optimizing their investigation resources by focusing their effort just on the most relevant behaviours, excluding the ones that are completely unregulated and which would require longer analysis times.

03

STRENGTHENED SECURITY RESEARCH AND INNOVATION

EU-CIP

EU-CIP: European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection

Habtamu Abie[1], Emilia Gugliandolo[2], Aleksandar Jovanovic[3], John Soldatos[4]

1. Norsk Regnesentral
2. Engineering Ingegneria Informatica S.p.A.
3. Steinbeis EU-VRi Gmbh
4. INNOV-ACTS Limited

1. Critical Infrastructure Protection (CIP): A Complex Technological and Policy landscape

In our contemporary and ever more interdependent and globalized world, Critical Infrastructure systems are the cornerstones of societies. They are complex, interrelated systems, networks and services essential for everyday life, businesses and social activities and underwrite the security of societies and communities [1]. Major shock events of all types, from natural hazards to industrial accidents, terrorist or cyber-attacks, have demonstrated the vulnerabilities of these critical systems. Their destruction, disruption or interruption could lead to cascading effects across sectors and sometimes across national borders. Vulnerabilities of Critical Infrastructure to a wide range of hazards and threats call for increased attention to Critical Infrastructure security and resilience [2]. Critical Infrastructure systems need to be resilient in the current landscape due to the growing complexity and interconnectivity of these systems, the increasing frequency and severity of disruptions, the criticality of these systems, and the high costs of disruptions. To ensure the resilience and the continuity of Critical Infrastructures, CI operators have deployed a host of different solutions, which range from security risk assessment and cyber security solutions to solutions that protect physical assets of critical infrastructures. The development of effective and innovative CIP solution is vital, given the growing sophistication of the CIs and the emerging challenges and threats that are recently faced by operators.

For instance, in an increasingly digitally interconnected world, CI operators need to deal with much more sophisticated cyber-security challenges than ever before. The latter include challenges (e.g., fake news and disinformation management) that were hardly considered in CIP solutions few years ago. Most importantly. CI owners and operators are nowadays conducting business in a highly unstructured, volatile and highly unpredictable environment, where asymmetric threats and other previously rate events are becoming the norm. This has been very evident during the last couple of years, when several CI operators had to confront challenges like the COVID19 pandemic outbreak, various large scale supply chain disruptions following the pandemic, as well as the recent Ukrainian war.

In this landscape, CI operators are forced to design and implement novel solutions that are not just reactive in nature, but rather able to predict and anticipate potential disruptions and security threats. Recent technological advances yield the development of such solutions viable and more pragmatic than few years ago. Nevertheless, the task of planning, design, developing, deploying and operating innovative solutions must take place in the scope of a complex landscape of i) multiple technological solutions, a sea of different standards, ii) a considerable number of regulations and directives, iii) a multi-stakeholder environment, and iv) a host of opportunities for combining diverse technologies into more complex, integrated and sophisticated solutions.

In this complex landscape, stakeholders need orientation regarding available solutions, gaps in current knowledge, limitations of the state of the art and the state of practice, as well as roadmaps for the development and deployment of innovative CIP solutions [3],[4].

2. The EU-CIP Mission

EU-CIP is a three-year Coordination and Support Action (CSA) that is funded by the European Commission. EU-CIP's vision is to establish a sustainable knowledge network of European CIP experts and stakeholders, which will provide knowledge, insights, foresights and guidance regarding research and innovation opportunities in the CIP domain. Specifically, one of the main objectives of the project is enhance Europe's analytical capability regarding research outcomes, technologies, and policies – foster data-driven evidence-based policy and innovation development. The activities that will lead to the accomplishment of this objective are conveniently called EU-CIP-ANALYSIS activities.

The EU-CIP-ANALYSIS activities will be implemented in a period of three years fol-

lowing the start of the project in October 2022. This paper presents some of the findings of the EU-CIP-ANALYSIS, notably findings produced following state of the art analysis and consultation with CIP stakeholders with the EU-CIP consortium and the ECSCI (European Cluster for Securing Critical Infrastructures) cluster i.e., a cluster comprising more than 30 of the most prominent European projects on security and critical infrastructures protection.

3. Preliminary Findings on Capability Needs and Capability Gaps

The EU-CIP Consortium members have identified the following CIP capabilities that are not adequately supported and covered by state-of-the-art solutions: Enhanced adaptability, Reduced Response Times, Increased Transparency, Improved Detection Capabilities, Improved risk and impact assessment capabilities, Better integration of Telco Security tools with Information Security Management tools, Solutions addressing cascading effects between different entities and states, Transformation of proactive and adaptive protection tools and methods to incorporate real-time functionalities, Better Exploitation of information from critical sensors towards augmented situation awareness, Risk prediction and anticipation, and Training, Reskilling and Upskilling.

Moreover, EU-CIP has also identified the following list of preliminary Capability Gaps (CG), which are partly linked to the above listed needs: Poor Automation, Lack of proper control of Interconnectedness, Poor Alignment of Resilience Indicators, Lack of agreed Standards-based stress-testing procedures, Problems with the classification of IoT Devices, Scalability in the Mitigation of Distributed Denial of Service (DDoS) attacks, Development and Deployment of AI-based systems, Lack of Holistic Security Management Systems, Gaps in Emergency Management Processes, Inability to cope with dynamically evolving threats, and Poor Awareness about modern CIP/CIR challenges.

These capabilities needs and gaps will be detailed in the extended version of the paper, while solutions that could help filling in the gaps will be outlined as well.

Acknowledgements

This project has received funding from the European Union's Horizon Europe- research and innovation programme under grant agreement No. 101073878. 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. Guidance notes on building Critical Infrastructure resilience in Europe and Central Asia, United Nations Development Programme. UNDP 2022
2.https://www.oecd-ilibrary.org/sites/76326acb-en/index.html?itemId=/content/component/76326acb-en
3. John Soldatos (ed.), James Philpot (ed.), Gabriele Giunta (ed.) (2020), "Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures", Boston-Delft: now publishers, http://dx.doi.org/10.1561/9781680836875.
4. John Soldatos (ed.), Isabel Praça (ed.), Aleksandar Jovanović (ed.) (2021), "Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry", Boston-Delft: now publishers, http://dx.doi.org/10.1561/9781680838237

EU-HYBNET

Innovations to counter Hybrid Threats. Results from the 2nd cycle of EU-HYBNET H2020 project

Souzanna Sofou[1], Dimitris Diagourtas[1], Antonis Kostaridis[1], Leonidas Perlepes[1], Aggelos Aggelis[1], Aleksandar Jovanovic, Somik Chakravarty[2]

1. Satways Ltd.
2. Steinbeis EU-VRi (European Risk & Resilience Institute).

Abstract

Hybrid threats can be defined as a coordinated and synchronised set of actions that deliberately target a country's vulnerabilities, using a wide range of means. Hybrid treats often seek to undermine fundamental democratic values and liberties [1]. The EU-HYBNET project brings together pan-European practitioners and stakeholders to identify the challenges in countering hybrid threats. This work presents the results of Work Package (WP)3: Surveys to Technology, Research & Innovations, which aims in monitoring and selecting innovative solutions that can be utilised to counter hybrid threats, based on the priorities identified for the latter in WP2 (Gaps & Needs of European Actors).

1. Exploitation of Critical Infrastructure Weaknesses and Economic Dependencies

1.1 Impact and Risk Assessment of Critical Infrastructures in a complex interdependent scenario

The cascading effects that can be caused after an attack on a Critical Infrastructure (CI) have raised concerns about CIs' interdependencies. However, the strategic dependencies have not been clarified, let alone the aggregated risk and impact implications. Understanding dependencies will help identify measures to reduce their impact, including diversifying production & supply chains, ensuring strategic stockpiling, and promoting production & investment in the EU.

The Innovation proposed is based on a paper by Weilan et al (2019) [2] and on the Critical Infrastructure Resilience Platform (CIRP) [3] developed by Satways Ltd. The paper by Weilan et al (2019) discusses a decision support approach for CI risk assessment with a holistic consideration of complexity, dual interdependency, vulnerability, and uncertainty. In this study, A) CI interdependency can be classified into three types, namely, geographic, functional, and stochastic. B) CIs can be regarded as system-of-systems to model the interdependent network structure and each CI can be viewed as a collection of components, where facilities are regarded as nodes and pipelines are treated as undirected edges that link facilities. C) Coupling effects are used to represent the influence of CI interdependency on the aggregated risk, and they are classified into complementary, redundancy, and zero.

The Critical Infrastructure Resilience Platform (CIRP) is a collaborative software environment. The essential elements for impact assessment are hazards, assets and the assets' fragility. Hazard is considered as the descriptive parameter, quantifying the possible phenomenon within a region of interest. The assets in a region exposed to hazards are defined by an inventory. Finally, fragility is the sensitivity of certain assets of an inventory when subjected to a given hazard. The implementation of such an algorithm in the CIRP Platform would include the following steps: i) Development of the asset taxonomy (including for example buildings, departments, infrastructure, servers), ii) Definition of interdependencies of the CIs (including geographic, functional, and stochastic), iii) Calculation of the vulnerability of all assets according to the fragilities defined iv) Selection of a threat scenario that can affect one or more assets v) Execution of the threat scenario and vi) Visualization of the scenario results. By implementing this algorithm, what-if scenarios can be studied for impact & risk assessment that can be used by practitioners for preparedness, that is, identifying measures to reduce the impact of interdependencies.

1.2 Resilience Tool (including RiskRadar)

The ResilienceTool is a web application for performing indicator-based resilience and functionality assessment for critical entities using a tested methodology based on composite indicators organized as a multi-level hierarchical checklist, known as dynamic checklists (DCLs). DCLs allow a dynamic combination of indicators recommended (for a particular sector/industry e.g., standards of IT systems in the transportation sector), and user-specific (e.g., policies applicable to a company or enterprise) indicators for monitoring, stress-testing and reporting of risk-resilience of cyber-physical systems. Further, the tool supports before/after analysis, assessment of existing interdependencies between infrastructures, as well as a multi-cri-

teria decision method (MCDM) based tool for appraisal of resilience enhancing investment options. The key concept of the methodology involves the "resilience" of an infrastructure which describes its ability to cope with potential adverse scenarios or events that can lead to significant disruptions in its operation or functionality.
The RiskRadar tool allows continuous and automated horizon scanning of "emerging risks" related to certain threats including hybrid threats that can potentially result in an "actual" risk in the medium to long term. The tool uses a natural language processing (NLP) algorithm to identify, locate and assess emerging risks by considering risks posed by threats based on factors including Environmental, Socio-political, Economic/Financial, Regulatory/Legal and Technological. It can extract textual data from a wide range of openly accessible documents from sources It has been effectively used for the identification and location of different types of perceived and real emerging risks/threats.

Acknowledgements
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054. 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. European Commission, Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats (2016)
2. Suo, W., Zhang, J., Sun, X.: Risk assessment of critical infrastructures in a complex interdependent scenario: A four-stage hybrid decision support approach, Safety Science 120, 692-705 (2019)
3. Kostaridis, A., Antonopoulos, S., Gkortsilas, D., Troullinos, M., Perlepes, L., Moutzouris M., Lykou, A., Koutiva, I., Karavokiros, G., Makropoulos, Ch., Chen, A.S., Vamvakeridou-Lyroudia, L., Gibson M., and Diagourtas, D., CIRP: A Multi-Hazard Impact Assessment Software for Critical Infrastructures. In: 2nd International workshop on Modelling of Physical, Economic and Social Systems for Resilience Assessment (2017)

EXERTER

EXERTER – what has come out of a five years network project on explosive threats

Anneli Ehlerding[1]

1. FOI, Swedish defence research agency

EXERTER, Security of Explosives pan-European Specialists Network, is a H2020 network project for explosives specialists connecting a wide community of practitioners, researchers, industry and government across the world.
During five years of the project, the aim has been to increase the exchange of information and be a link between practitioners, academia, industry, research organisation and other stakeholders in the field of explosives. In discussions within EXERTER, areas in need of development, or recommendations and ideas for improvements, have been highlighted and put forward. EXERTER focus on the explosives threats in various situations, but are also extending the discussions to a wider view on countering current and emerging terrorist threats.
The main objectives of EXERTER have been to:
• Provide solutions to practitioners in the field by extrapolating terrorist threats and attack strategies from recent incidents and matching these with existing and emerging technologies and tools. That is, by analysing future threats together within the community, analysis of upcoming tools and their relevance can be made, and it can lead to development in collaboration with practitioners.
• Ensure the practice-relevance of R&D activities by defining end-user requirements and pinpointing existing capability gaps. That is to say, by involving the practitioners in the process and connect them to the product developers, developing tools which do not quite meet the needs can be avoided.
• Support practitioners as well as academia, developers and innovators in their search to find potential industrial partners who have the capability to exploit the innovations into products. This is an important part, where the network plays a role to support exploitation.

• Enhance practitioner's operability by supporting standardisation and certification bodies as well as regulators with standardisation and certification priorities in order to facilitate comparison of SoE products and procurement. Often, in the interaction between the different actors, ideas, suggestions and challenges are brought up, and by lifting these, processes have a chance of improving.
• Enable a long-term cooperation among explosives specialists in the security area beyond EXERTER. The community has throughout the project expressed a true need for such a network and cooperation.

Each year, EXERTER has defined a theme, or a set of scenarios, and used it as a basis for discussions around needs, requirements, gaps and ideas with practitioners and other stakeholders. Based on these discussions, research findings and issues related to certification and standardisation connected have been identified and brought up for discussion and presentation to the community. During the five years of EXERTER the themes have covered vehicle-borne IED:s, person-borne IED:s, explosive threats to public transport systems, criminal use of explosives, and influences on EU civil security emanating from conflict zones. Throughout the work in EXERTER a large part of the course of events is covered, from Prevent, where for example production is aggravated, and Detect, where the threat or connected items are detected , to Mitigate and React, where measures to limit the effects and to handle the post blast scene are covered, respectively.

Figure 1. *The counter-attack domains, covering most of the course of event for an attack.*

Each year, workshops have been held with practitioners, where they have had the chance to discuss their needs, ideas, recommendations, and experiences with the rest of the community. These workshops have been highly appreciated, and increased interaction within the community with both practitioners and researchers.
In EXERTER there has also been a review of research initiatives which can be relevant for the different scenarios, in order to both highlight promising or interesting research to the network, and to identify areas where research could increase knowledge and capabilities. Standardisation and certification issues connected to the threat from explosives have also been reviewed, and suggestions or challenges have been raised.
Throughout all of this work, areas which were raised in discussions with practitioners were used for further discussions and reviews. For example, in the Vehicle-borne IED scenario, based on the Oslo bombings in 2011, research to prevent manufacturing of explosives and physical barriers were highlighted, for the Explosives in public transport-scenario, access to commercial explosives, explosives detection systems and checkpoints were some of the areas of importance. During the work on Criminal use of explosives, some of the highlighted areas concerned pyrotechnics, organised crime groups, post-blast analysis, and support to legal prosecution. For the final year, working around Influences on civil security from conflict zones, discussions have been ongoing around for example smuggling, pyrotechnics, explosive remnants of war, and future threats. The discussions in EXERTER around all of these issues have been ongoing through multiple EXERTER webinars, workshops, annual conferences and other meetings within the community.
Some issues have been raised and discussed repeatedly in these workshops, but from slightly different angles. Examples are pyrotechnics education and regulations, border control regulations, detection systems, and work on forensics and support to prosecution. It has been clear through the discussions that in those areas there remains much work in order to increase the security and harmonise the processes across Europe.
Throughout the five years of networking, some lessons have been learnt on how to increase interaction with the community and create a lasting network. Primarily, as simple as it may sound, there has to be a need for a network - a bottom up approach, where the needs and interests of the community drives the network is an important basic principle. It has also shown that it is important to grow the network in a balanced manner, and to build trust amongst the participants. Keeping the subjects and discussions up to date and relevant is another important baseline, where EXERTER has used the up-to-date themes and scenarios, developed in collaboration with the practitioners, each year.. Collaboration with other European projects are also an important factor, in order to connect to other work and share expertise when possible. It is clear that EXERTER has played an important role in the community, as a platform to gather expertise, discuss relevant topics and share knowledge on explosive threats to other communities and networks.

Firelogue

Lessons on Fire by Firelogue platform: gathering and promoting Wildfire Risk Management project results

Mariza Kaskara[1], Sofia Oikonomou[2], Claudia Berchtold[3], Haris Kontoes[1]

1. National Observatory of Athens, Operational Unit BEYOND Centre for Earth Observation Research and Satellite Remote Sensing IAASARS/NOA
2. EDGE in Earth Observation Sciences
3. Fraunhofer Institute for Technological Trend Analysis

1. Introduction

Firelogue, as a CSA and EU project, brings together expertise from all around Europe when it comes to Wildfire Risk Management (WFRM). Through the development of a platform, the connecting dimension of Firelogue focuses on the collection of knowledge, insights and solutions from the successful Innovation Actions[6], and the consolidation of this knowledge, such as of the technologies and derived services that will be developed by the IAs.

2. Firelogue Project

Firelogue's primary objective is to facilitate Wildfire Risk Management (WFRM) by bringing together experts from all over Europe. Firelogue aims to create a dialogue and empower the WFRM community to tackle current and future wildfire challenges, acting as an exchange enabler of knowledge through the aggregation of experience and best practices of all engaged stakeholders.
Firelogue project aims to support and coordinate the consolidation of knowledge from the successful wildfire risk related Green Deal Innovation Actions as well as from the wider community. It integrates findings across stakeholder groups and fire management, and promotes discussion via forums and workshops, leading to exchange among a large range of stakeholders. Moreover, Firelogue's mission is to create a conducive environment that fosters communication within the WFRM community and society, as well as retain and share the knowledge and experiences gathered alongside the demonstration of innovative actions and products.
More specifically, Firelogue aims to:
• Stimulate and provoke the cooperation and synergies of the different actors in the framework of the WFRM community;
• Empower the WFRM community to face the current and future wildfire challenges;
• Engage all relevant target groups to provide inputs and learn from each other's best practices and expertise;
• Raise awareness among practitioners, civil society and beyond about the great advance and importance that Firelogue represents to be able to construct a smooth and good dialogue within the wildfire sector;
• Support relevant policy makers to offer more knowledge and security for the civil society.

6. FIRE-RES, SILVANUS, TREEADS

3. Lessons on Fire powered by Firelogue Platform

In order to achieve the aforementioned objectives and in the prospect to create an online WFRM Community, Firelogue has developed a platform called "Lessons on Fire powered by Firelogue" (LoF by Firelogue) in collaboration with the Pau Costa Foundation, based on their existing and well-established platform "Lessons on Fire". After the completion of the project, the Pau Costa Foundation will continue its efforts to sustain the LoF by Firelogue platform, thereby ensuring its sustainability.
The LoF by Firelogue platform serves as a valuable resource for the WFRM community, providing a central location for sharing knowledge, news, events, promotional platforms and resources related to WFRM. The platform is open to other fire-related projects, and registered users can upload their own content, making it a collaborative effort to improve WFRM. The platform, among other, provides opportunities for users to connect with other professionals, stay informed about the latest fire-related events and news, access technical results, WFRM measures, case studies, and fire-related documents. Registered users can upload their own fire-related content, giving the opportunity to fire-related projects and WFRM stakeholders to upload their results, documents, events, and news.
In detail, LoF by Firelogue provides many features with the goal to create an online WFRM Community.
The first/frond page contains the new combined logo of Firelogue and the precursor "Lessons on Fire" and a small reference to the content of this platform. The

visitor scrolls to the "About" section, where a more detailed description of the platform is given and three concepts that are frequently used within the platform are referred. These concepts are commonly referred to as the "Three Phases of Fire," the "WFRM Community," and the "#EUFireProjectsUnited." The user is encouraged to register and become a member and then to use the advantages of a registered member; uploading a file to the Library or an Event to the calendar, features that will be explained below.

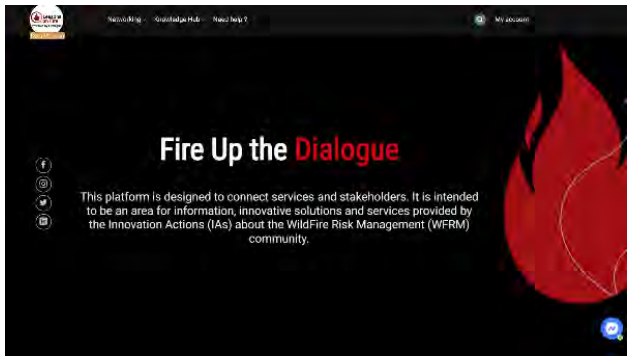


Figure 1: *Landing page*

Lessons on Fire powered by Firelogue have two main pages; Networking & Knowledge Hub.
On the Networking page, the users can find more about EU Dissemination platforms to boost their project's results, stay up to date and in touch with other scientists and stakeholders, find out about fire-related events (conferences, workshops, etc.), and the latest news. By becoming registered users, they have the advantage of uploading their information on the networking page and sharing documentation with the WFRM community. On the Knowledge Hub page, the users can find a global map of fire-related case studies, a Technology Mall with fire-related technologies as well as other WFRM actors, approaches, actions, strategies and Standard Operating Procedures. The user can also find a list of existing platforms with fire-related topics. There is also a "Library" of fire-related articles and scientific research papers, to which the users can upload their work and become part of the WFRM community. Results, recommendations and papers from Firelogue's WGs will be also uploaded in the LoF by Firelogue "Library".

4. Impact

The platform is designed to have a significant impact on the WFRM community by

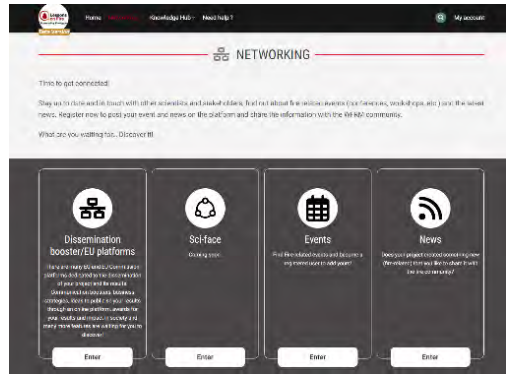


Figure 2: *Networking function*

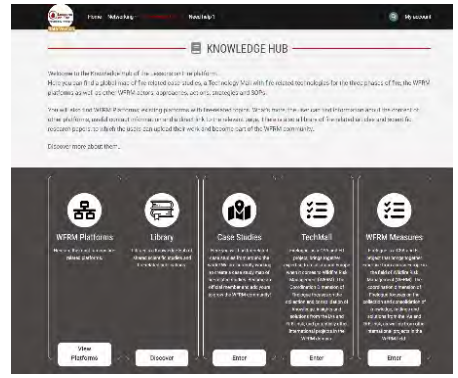


Figure 3: *Knowledge Hub function*

providing a space for collaboration, knowledge sharing, and networking. Through the platform, members of the community can connect with experts in the field, access valuable resources, and stay up-to-date on the latest research and best practices. One of the most significant benefits of the platform is the ability for members of the WFRM community to create their own content and connect with each other. This collaboration allows for the sharing of ideas and experiences, ultimately leading to more effective and efficient management of wildfires. By bringing together experts and practitioners from around the world, the platform has created a truly global community focused on addressing the complex challenges of wildland fire management. In addition to networking, the platform has also played a crucial role in knowledge sharing. Members can access a wide range of resources, including research articles, case studies, and training materials, all of which help to advance the field of WFRM. By promoting the dissemination of information, the platform has helped to improve the overall quality and effectiveness of WFRM practices.

5. Conclusion

Overall, Firelogue and LoF by Firelogue Platform, referring to all stakeholders, are crucial resources for the WFRM community, policymakers, and civil society to face the current and future wildfire challenges. By creating a dialogue and empowering the community, Firelogue is making significant contributions to the Just Transition concept and the overall effort to mitigate the impacts of wildfires.
Visit Firelogue's platform to explore those features: https://lessonsonfire.firelogue.eu/

Acknowledgements
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101036534. 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.

MEDEA

Policy recommendations for combating new trends in drug trafficking

Freideriki Makri[1], Genny Dimitrakopoulou[1], Nikolaos Kapsalis[1], George Kokkinis[1]

1. Centre for Security Studies (KEMEA)

1. Introduction

Organised Criminal Groups (OCGs) involved in drug trafficking are becoming polycriminal, since they use their profits to fund other forms of criminal operations, and even terrorism. The current paper focuses on the challenges faced by Law Enforcement Agencies (LEAs) in their operations against drug trafficking and moves to a list of recommendations about the intelligence exchange between EU Member States (MSs), lawful interception of communications, and cryptocurrencies.

2. The Challenge

Tackling drug trafficking remains one of the EU's priorities in the fight against serious and organised crime [1]. The last years, OCGs are advancing their smuggling methods with the advantages that new Information and Communication Technologies offer [2], leaving LEAs is a disadvantageous position, by making existing tools and procedures outdated. Additionally, the accessibility of illicit drugs via social media platforms, apps, online marketplaces [3], as well as the use of online payments, including cryptocurrencies, and encrypted digital communication is not effectively monitored nor analysed in a coordinated way. Notwithstanding, several challenges have more legal grounds, instead of technological.

3. MEDEA findings

The Mediterranean and Black Sea network of practitioners (MEDEA) developed a realistic trafficking scenario to study the challenges of practitioners and other stakeholders. The scenario was focused on the trafficking of heroin, Europe's most

used illicit opioid4, from Asia to EU through the Balkan route which is the main heroin trafficking corridor linking production countries to European market with an annual market value of some $20 billion [5]. The scenario analysis revealed several security gaps [6] that were further analysed to formulate the challenges faced by security practitioners. Further interaction and processing of findings pave the way to form recommendations that benefit security practitioners.

3.1 Interconnect existing EU databases.

The importance of the information and intelligence exchange between MSs with the aim of combatting serious crime is already known and various steps have been taken to enhance the cooperation and information sharing [7]. Databases and frameworks to accompany their usage have been developed for enhancing data sharing like the European Arrest Warrant, the European Criminal Records Information System, and the Customs Advance Cargo Information System. The EU bodies should move towards the interconnection of the existing EU databases used by practitioners and the unification of their frameworks under one single framework that will constitute the basis of a more structured information sharing, taking into consideration the national legislations.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 787111. 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. Europol, EU Policy Cycle – EMPACT, https://www. europol.europa.eu/crime-areas-and-trends/eupolicy-cycle-empact 2 UNODC
2. UNODC, Organised Crime Module 3: Drug Trafficking, https://www.unodc.org/e4j/zh/organized-crime/ module-3/key-issues/drug-trafficking.html

MULTIRATE

MULTIRATE

MultiRATE: EU R&D Readiness Level Evaluation Framework

Dimitrios Kavallieros[1], Christos Voulgaris[1], Katerina Valouma[2], Ilias Gkotsis[2], Theodora Tsikrika[1], Stefanos Vrochidis[1], Ioannis Kompatsiaris[1], Dimitris Diagourtas[2], Antonis Kostaridis[2]

1. Center for Research and Technology Hellas-CERTH, Information and Technologies Institute
2. Satways Ltd

1. Challenge

Plenty of different metrics dedicated to the evaluation of the overall maturity of products and systems exist nowadays. Even though significant efforts have been made to integrate widely used frameworks, methodologies and indicators for measuring the maturity of products and systems, it has not been any framework or methodology that integrated multiple Readiness Level (RL) domains under a holistic framework and, most importantly, tailored to security solutions. As a result, the development of a robust scaling framework is of utmost importance, in order to achieve the improved cross-disciplinary assessment of the maturity of novel technologies (developed for security practitioners) based on a harmonised framework. Moreover, there is a need for more efficient use of maturity assessment frameworks to convey technology readiness, synchronize parallel projects, forecast deployment, and support decision-making in security investment planning.

2. MultiRATE solution and approach

MultiRATE will conduct research in multiple fields to create a solid ground for the development of the holistic, homogenous and harmonised RL evaluation methodology. The fields of research include the following: Technology (TRL), Societal (SRL), Security (SecRL), Legal, Privacy and Ethics (LPERL), Integration (IRL), Commercialisation (CRL) and Manufacturing (MRL). In each field, appropriate indicators will

be identified per level (e.g. RL1-9) to accurately evaluate the solutions developed for the security domain. Where appropriate, the consortium will identify indicators for both LEAs and non-LEAs security practitioners. Moreover, the project aims to evaluate solutions in all aforementioned fields, by developing a unique methodology and indicators as each field measures different aspects, assets and has different objectives. MultiRATE will integrate the aforementioned RLs under a Holistic RL evaluation methodology and tool for security related solutions. The EU R&D community will take advantage of the developed solution, harmonising the approach taken from all R&D projects, initiatives and more.

MultiRATE solution will be designed in an agile and robust manner, followed by repeated tests and validation steps in multiple domains (e.g. Cybersecurity, Border Management, Fight against Crime and Terrorism etc.), maximizing its accuracy.

As it was described before, MultiRATE will develop RL calculation methodologies and indicators for seven domains and it will produce a holistic RL indicator.

In the following sections, we will focus on three specific RLs, the TRL, the MRL and finally the CRL.

2.1 Technology Readiness Level

NASA introduced the TRL in the 70's and it had seven levels, which were formally defined in the late 80's focused on space missions and the relevant technological requirements and components. In the 90's NASA altered this to a nine level scale (the lowest level is TRL 1 while the highest is TRL 9) and in 2013 the International Organization for Standardization produced the ISO 16290:2013 standard (Space systems — Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment) [1]. The focus of the TRL was to evaluate the maturity of developments in space technology. The TRL was introduced in EU-funded projects in 2014 [2], adapting the term of each level to fit the Horizon 2020 programme, keeping though the overall meaning of each level. Nevertheless, no assessment guideline or criteria per level were developed, thus each R&D consortium was assessing the TRL of their developed solutions based on internal and vague procedures. MultiRATE will design a concrete methodology to assess the maturity of solutions designed and developed under the horizon Europe Cluster 3: "Civil security for society" based on a set of indicators per level. The indicators will work as the criterion of a concrete methodology assessing if a technology has reached a TRL.

2.2 Manufacturing Readiness Level

In 2003, the Government Accountability Office (GAO) recommended in GAO Report 03-476 [3], established cost, schedule, and quality targets for product manufacturing, in order to obtain process maturity. The report suggests that design and manufacturing knowledge should be obtained early in product development for a product to be successful. In response, the Joint Defense Manufacturing Technology Panel developed MRL definitions as well as Manufacturing Readiness Assessments (MRAs). This MRL scale helps program managers assess manufacturing risks, but also facilitates the identification of areas that require additional management attention or investment. Manufacturing readiness is as important to the successful development of a system as the readiness and capabilities of the system. Though MRLs were created from the manufacturing perspective to evaluate —the manufacturing readiness of a product and supplement existing TRLs, they, too, have limitations. A limitation of the MRLs is that the lower MRL levels can be difficult to correlate to corresponding TRL numbers due to the technology immaturity. MultiRATE will adjust existing methodologies and will develop indicators specifically for security-related technologies under EU R&D funded programs. Furthermore, it will seek to harmonise the levels of the MRL with the TRL and the rest of the RLs designed in the project.

2.3 Commercialization Readiness Level

The Commercialisation Readiness Level (CRL) framework assesses various indicators, which influence the commercial and market conditions beyond just the technology maturity. This enables key barriers to be addressed to support the commercialisation of technology. CRL refers to how ready a product or service is to take to the market, as a commercial offering for a group of customers. CRL is a more recent concept, and definitions and operationalization of commercialization readiness are therefore far less widely accepted and solid than TRL. However, the focus on market readiness has become increasingly prevalent, as e.g. expressed by Horizon2020s sharpened focus on the market aspect of product development (CloudwatchHub,2020 [4]). MultiRATE will consider the limited existing methodologies, combining and enhancing them with best practices and lessons learned in the commercialisation domain, finally developing indicators and assessment framework tailored to the needs and peculiarities of EU R&D funded security related technologies. Furthermore, it will seek to harmonise the levels of the CRL with the TRL and the rest of the RLs designed in the project.

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 REA. Neither the European Union nor the granting authority can be held responsible for them.

References
[1] International Standard Organisation, ISO 16290:2013 Space systems — Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment, International Standard Organisation, 2013.
[2] J. Banke, "Technology Readiness Levels Demystified," 7 August 2017. [Online]. Available: https://www.nasa.gov/topics/aeronautics/features/trl_demystified.html. [Accessed 6 May 2023].
[3] U. S. G. A. Office, "GAO-03-476 Defense Acquisitions: Assessments of Major Weapons Programs," Washington, D.C., May 2003.
[4] CloudWATCH2, "Think Cloud Services for Government, Business and Research," 2016. [Online]. Available: http://www.cloudwatchhub.eu/.

NOTIONES

NOTIONES - interacting network of intelligence and security practitioners with industry and academia actors

Maria Ustenko[1], Giulia Venturi[1]

1. Zanasi & Partners

1. Network of security and intelligence practitioners
NOTIONES is an EU-funded project that aims to establish an interacting network of security and intelligence practitioners with industry and academia actors to promote innovation and collaboration in the field of security research. The project brings together a diverse group of experts from various sectors to develop innovative solutions to emerging security threats.
The NOTIONES project recognizes that traditional security approaches are no longer adequate to address the complex and rapidly evolving nature of security threats. The project therefore seeks to promote a more collaborative and interdisciplinary approach to security research, involving experts from academia, industry, and security and intelligence agencies.
One of the key objectives of NOTIONES is to foster innovation in security research. This is achieved through a variety of activities, including research monitoring, technology scouting, and the development of innovative tools and methodologies for security practitioners. The project also provides a platform for knowledge sharing and collaboration, allowing participants to exchange ideas and best practices and to develop new approaches to security challenges.
Another important aspect of NOTIONES is its focus on promoting ethical and legal standards in security research. The project aims to ensure that all research and development activities are conducted in accordance with ethical and legal principles, and that the resulting technologies and methodologies are designed with privacy and human rights considerations in mind.

Through its various activities and initiatives, NOTIONES is helping to shape the future of security research by promoting collaboration, innovation, and ethical standards. The project aligns with the EU's broader objectives of promoting innovation, competitiveness, and security across Europe. Through its engagement with industry and academia actors, NOTIONES is helping to drive forward the EU's innovation agenda and to position Europe as a leader in the field of security research. The project has already made significant contributions to the field, and its ongoing efforts are likely to have a major impact on the development of new approaches to security challenges in the years to come.

In conclusion, the NOTIONES project is an important initiative that is helping to bridge the gap between security and intelligence practitioners, industry actors, and academia, in order to develop innovative solutions to emerging security threats. By promoting collaboration, innovation, and ethical standards, NOTIONES is helping to shape the future of security research and ensure that our societies remain safe and secure in the face of ever-evolving security challenges.

Acknowledgements

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

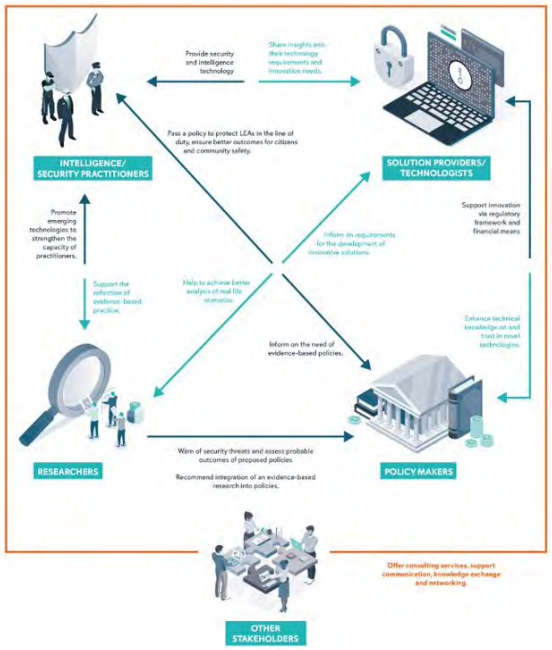


Figure 1. *Ecosystem of security and intelligence practioners.*

04

CRITICAL INFRASTRUCTURES RESILIENCE AND SMART CITIES

ATLANTIS

Improved Resilience of Critical Infrastructures Against Large Scale Transnational and Systemic Risks

Gabriele Giunta[1], Jolanda Modic[2], Theodoros Semertzidis[3], Theodore Zahariadis[4]

1. Engineering Ingegneria Informatica Spa
2. Institute for Corporative Security Studies
3. Centre for Research and Technology Hellas
4. Synelixis Solutions SA

1. Background

Reliable operation of Critical Infrastructures (CIs) is a pre-requisite for the integrity and resilience of vital elements in our society that help to ensure the security, well-being, and economic prosperity of Europe, its citizens, and businesses. However, CIs have become very complex, operating in a rapidly evolving societal, technological, and business environments. Growing digitalisation generates new vulnerabilities, including those carried through people and employees, either intentionally through insider threats or through human errors and social engineering. Moreover, since CIs are becoming more interconnected and reliant upon one another, disruptions in one CI can have severe and long-lasting cascading effects in other CIs that are essential for the continuity of critical societal and economic activities, even in multiple sectors and countries. This increases the attack surface as well as the scale and significance of the impacts of attacks. In this emerging safety-security landscape, European Critical Infrastructure (ECI) are increasingly becoming the targets of new categories of hybrid threats and attacks powered by technological innovations. However, large-scale vulnerability assessment and systemic risks analysis of ECI, considering the risks derived by major man-made or natural hazards and complex Cyber-Physical-Human (CPH) threats as well as consequences of the entire system collapse, have never been addressed before.

ATLANTIS evaluates and addresses systemic risks against major natural hazards and complex attacks that could potentially disrupt vital functions of the European society. The mission of ATLANTIS is to improve the resilience of the interconnected ECI exposed to ever evolving, existing and emerging, large-scale, combined, CPH threats and hazards. By providing future-proof, sustainable security solutions, ATLANTIS supports public and private actors in guaranteeing continuity of vital operations while minimizing cascading effects in the infrastructure itself, the environment, other CIs, and the involved population.

2. ATLANTIS concept and pilots

The key challenges of security, resilience and privacy need to be encapsulated in a user-driven three dimensional approach in order to achieve the strategic objectives that lead to holistic and systemic security. The three traditional security elements of technology, processes, and humans implement a Technology-Humans-Process symbiotic relationship, supplemented by a fourth "node" of collaborative security strategy to create a 3D ATLANTIS security model. In this "pyramid", the technology is specifically assigned to develop and implement tools focused on the protection of CI, which requires advancing the technology itself, but also improving the collaboration between vendors and users to achieve optimal security. ATLANTIS utilizes and extends technology, processes and humans though it primarily focuses on the collaborative security to offer cross-CI systemic security.

ATLANTIS will be validated and demonstrated in 3 large-scale cross-border and cross-sector pilots (LSPs), with a focus on improving the security of the information exchange inside individual CIs, across CIs in a national security environment, and across borders between CI operators:

LSP#1: Cross-Border/Cross-Domain LSP in Transport, Energy, and Telecoms - Validation in (i) multimodal cross-country transport encompassing sea transport with two international seaports, rail transport with two national railway operators, and road transport with a national highway operator, (ii) energy (oil), and (iii) telecoms in four neighbouring countries: Slovenia, Croatia, Italy, and France.

LSP#2: Cross-Domain LSP in Health, Logistics/Supply Chain, and Border Control - Validation in (i) the health sector covering physical protection of hospitals and cybersecurity of Electronic Health Records with a group of 3 hospitals in Greece, (ii) logistics/supply chain covering logistics and Enterprise Resource Planning (ERP) platforms in Greece and Cyprus, and (iii) border control with a focus on the Schengen II Information System for border control of Cyprus, Greece, and Croatia.

LSP#3: Cross-Country LSP in FinTech/Financial - Validation in the financial sector

covering cybersecurity incidents and systemic threats with an independent investment house, a bank, and technology providers specialised in developing technology, infrastructure, and business solutions for the financial sector.

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

ERATOSTHENES

ERATOSTHENES - Secure management of IoT devices lifecycle through identities, trust and distributed ledgers

Konstantinos Loupos[1], Harris Niavis[1], Antonio Skarmeta[2], Jesus Garcia[2], Angel Palomares[3], Hui Song[4], Rustem Dautov[4], Francesca Giampaolo[6], Dimitri Van Landuyt[7], Sam Michiels[7], Blaz Podgorelec[8], Christos Xenakis[9], Michail Bampatsikos[9], Dimitrios Sivridis[10], Konstantinos Krillakis[10]

1. INLECOM INNOVATION
2. UNIVERSIDAD DE MURCIA
3. ATOS IT SOLUTIONS AND SERVICES IBERIA SL
4. SINTEF AS
5. ENGINEERING - INGEGNERIA INFORMATICA SPA
6. KATHOLIEKE UNIVERSITEIT LEUVEN
7. TECHNISCHE UNIVERSITAET GRAZ
8. UNIVERSITY OF PIRAEUS RESEARCH CENTER
9. EULAMBIA ADVANCED TECHNOLOGIES

ERATOSTHENES project is driven by recent security challenges of IoT networks being today embedded into our day to day lives. The high increase of connected devices, their inhomogeneous nature, high penetration, as well as different manufacturing and vendor characteristics have created a vast attack surface that is prone to increase in the next years. This has already created challenges such as: confidentiality access control, privacy for users and things, devices' trustworthiness and compliance that require lifecycle considerations of IoT devices and networks. ERATOSTHENES will devise a novel distributed, automated, auditable, yet privacy-respectful, Trust and Identity Management Framework intended to dynamically and holistically manage the lifecycle of IoT devices, strengthening trust, identities, and resilience in the entire IoT ecosystem, supporting the enforcement of the NIS directive, GDPR and Cybersecurity Act. ERASTOSTHENES will leverage breakthrough

solutions: (a) the first-ever enclosure of cybersecurity features in IoT devices; (b) decentralized identity management mechanisms to conciliate requirements of self sovereignty and privacy preservation in a distributed/transparent trust model along with disposable identities; (c) self encryption/ decryption at device-level; (d) threat-analysis models based on federated learning and edge execution; (e) collaborative IoT threat intelligence sharing across ledgers to adapt detection/defense mechanism; (f) integration of Physical Unclonable Functions in trust framework and distributed ledgers. The overall vision of ERATOSTHENES is to provide core cybersecurity features to be adopted by manufacturers as baseline certification elements in the production of devices and throughout their entire lifecycle. The solution will be validated in 3 industrial cases: Automotive, Health and Industry 4.0.

ECSCI

European Cluster for Securing Critical Infrastructures

Ilias Gkotsis[1], Habtamu Abie[2]

1. Satways Ltd
2. Norwegian Computing Center

Abstract

The European Cluster for Securing Critical Infrastructures (ECSCI) is a cluster of H2020 and Horizon Europe research and innovation projects in the field of cyber-physical protection of critical infrastructures (CIP). Its main objective is to highlight and elaborate on emerging innovative solutions to security issues via cross-projects collaboration and innovation. ECSCI members share knowledge and best practices about CIP in different sectors. The cluster focuses on research and innovation outcomes on the protection and security of critical infrastructures and services, respecting the different approaches, CI sectors focusing, target audience, etc., between the projects, while establishing tight and productive connections with closely related or complementary ones.

Joining forces and clustering activities towards enhancing the resilience of critical infrastructures

Modern critical infrastructures (or "critical entities" as now defined in the new EU-CER Directive) are becoming increasingly complex, turning into distributed, large-scale cyber-physical systems. Cyber-physical attacks are increasing in number, scope, and sophistication, making it difficult to predict their total impact. Thus, addressing cyber security and physical security separately is no longer effective, but more integrated approaches, that consider both physical security risks and cyber-security risks, along with their interrelationships, interactions and cascading effects, are needed to face the challenge of combined cyber-physical attacks. Addressing them successfully, need coordinated and integrated responses, which

must be disseminated and exploited further to the EU funded projects' frameworks or individual research studies' reports, through raising awareness initiatives.
In this direction, the main objective of the ECSCI cluster is to create synergies and foster emerging disruptive solutions to security issues via cross-projects collaboration and innovation. Research activities focuses on how to protect critical infrastructures and services, highlighting the different approaches between the clustered projects and establishing tight and productive connections with closely related and complementary EU funded projects. To promote the activities of the cluster, ECSCI will organize international conferences, and national or international workshops, involving both policy makers, industry and academic, practitioners, and representatives from the European Commission.
ECSCI, as a collaborative ecosystem on critical infrastructures protection, collaborates on the following areas:
• **Scientific collaboration** in the form of joint workshops and conferences, and co-writing of scientific publications;
• **Technical collaboration** such as sharing approaches on cyber-physical security, risk assessment, and predictive analytics;
• **Communication and dissemination** of cluster's activities and outputs through a common web and social media presence, and organization of joint events;
• Building and fostering **stakeholders' alliance** (mobilisation of local ecosystems);
• **Marketplace extension** of members' products and services across various sectors and stakeholders.

As a result, collaboration and knowledge sharing among experts in the field is critical for **ensuring the security and readiness of European critical infrastructures and services.** In this direction, the ECSCI cluster tries to consolidate and reflect a European approach by engaging in various common activities:
• **Contribution to standards and regulations** on the protection of Critical Infrastructures;
• **Joint scientific publications,** including a broad spectrum of respective books;
• **Workshops and events on critical infrastructure protection,** with keynote speakers from policy making, academic and industrial sector;
• **A platform for combined safety and security for European Critical Infrastructures.**

References

1. ECSCI official website, www.finsec-project.eu/ecsci
2. Consolidated Proceedings of the 1st ECSCI Workshop on Critical Infrastructure Protection, www.steinbeis-edition.de/shop/out/pictures/media/218957.pdf
3. Consolidated Proceedings of the 2nd ECSCI Workshop on Critical Infrastructure Protection, www.steinbeis-edition.de/shop/out/pictures/media/9783956632853.pdf
4. Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry, www.nowpublishers.com/article/BookDetails/9781680838220
5. Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures, www.nowpublishers.com/Article/BookDetails/9781680836868

HERON

Supporting maintenance tasks and upgrading roadworks through an integrated automated system

Ilias Gkotsis[1], Aggelos Aggelis[1], Leonidas Perlepes[1], Antonis Kostaridis[1], Theodora Karali[2], Dimitrios Bilionis[2], Stefanos Camarinopoulos[2], Yannis Handanos[3], Solon Molcho[3]

1. Satways Ltd
2. RISA Sicherheitsanalysen GmbH
3. Olympia Odos

1. Introduction

Of all transport infrastructure, but also public assets, road infrastructure tops the list. Roads are crucial for economic development and growth, providing access to education, health, and employment. The maintenance, repair and upgrade of roads is one of the most important parts for their high level service provision.

At a time of zero tolerance (zero accidents, zero operating restrictions, etc.), it is increasingly necessary to control risks and to improve the knowledge of the condition of structures in order to organise preventive and/or predictive maintenance that minimises risks at an acceptable cost. Instrumentation, particularly in the context of preventive monitoring, is an important tool, as are risk analysis approaches. It allows, in this case, to better understand the behaviour of structures, to know their condition, and thus to provide reliable input data for a robust risk analysis.

In order to meet the above needs, HERON project will develop an integrated automated system to perform maintenance and upgrading roadworks, such as sealing cracks, patching potholes, asphalt rejuvenation, autonomous replacement of CUD elements and painting markings, but also supporting the pre/post-intervention phase including visual inspections and dispensing and removing traffic cones in an automated and controlled manner. In turn, this will reduce accidents, lower maintenance costs, and increase road network capacity and efficiency.

2. HERON solution

To coordinate maintenance works, HERON will design an autonomous ground robotic vehicle that will be supported by autonomous drones. Sensors and scanners for 3D mapping will be used in addition to artificial intelligence (AR) toolkits to help coordinate road maintenance and upgrade workflows. The above components will be combined with several other technologies, which will all be integrated into a Incidence management & Decision Support System (IMS&DSS), with Common Operational Picture (COP) capabilities. The aim is to provide to the operators and field crew all the information required to organize their operational procedures and execute successful road inspection and decision-making activities.

The IMS will generate and share a COP among Road Infrastructure (RI) personnel and relevant road authorities permitting the collaborative response of all involved relevant local and regional partners when needed. For maintaining the effective communication, facilitate the process and to ensure unity of effort, the IMS, will utilize protocols for multi-level and multi-actors' interaction.

The COP will act as the central and virtual representation of the HERON Robotic platform controller, providing to the Robot operators and decision-makers of the RI companies all the information required to organize successfully their tasks. The various COP elements will be decomposed into information layers and categories in order to allow for a flexible system that permits the "need-to-know" principle as different users and roles are envisaged to interact with the HERON tools .

The AR system will provide real-time visual information on the surrounding environment of the robot operators. The AR app software will visualize the amount of the existing defects (automated detection of pavement defects and classification of severity) and will use overlays of 3D models to display possible hidden structural elements which can affect the maintenance process or additional damages. Display of functional elements will be available through appropriate commands too.

The IMS&DSS will be interconnected with HERON Middleware and support the specifications and business logic of the use cases. The Middleware will ensure data integrity by accepting and storing sensor data from trusted sources, allowing access only to authorized requests. It includes a tailored policy-based management frame-

work along with suitable enforcement mechanisms dealing with data encryption, access control, privacy and anonymity. Furthermore, this block includes intrusion detection and prevention mechanisms, such as tools dealing with protocol analysis, detection of anomalous behaviour, security events, intrusion detection, vulnerability assessment and honeypots. It also includes knowledge repositories and distributed threat registries. The appropriate interfaces/protocols for the communication with the different data sources and user services will be created. The module will handle seamlessly aspects such as time synchronization, scheduling, selection of communication paths, fault-tolerance and traffic shaping.

3. End user needs and expectations – the Greek pilot case

The aforementioned components and the HERON solution as a whole, will be tested, validated and evaluated, with respect to the infrastructure operators' expectations and respective KPIs.

One of the main HERON road operators is that of OLYMPIA ODOS in Greece, which provides operation and maintenance services, such as toll collection, traffic management & safety and routine maintenance. The main needs include:

• to prevent its early wear and restore any damage, wear or malfunction may be presented in an effective and efficient way;
• to operate at a high level of service and to keep a smooth and continuous traffic flow under normal operation conditions, maintain these flow conditions and minimize the delays;
• to zero the incidents with implication of its personnel;
• to save natural resources, prevent pollution and reduce its negative environmental impact, and protect third parties' assets, in the areas of the company's operation.

Under this framework the HERON's system is expected to:

• improve the cost of maintenance activities, by reducing mainly the required human resources;
• reduce the time period of road/lane closures and the relevant road users' annoyance;
• minimise personnel's exposure to risks both due to maintenance activities and adjacent traffic;
• minimise environmental pollution and ensure sustainability.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 955356. 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. D2.1 | End-user needs and KPIs report. www.heron-h2020.eu/wp-content/uploads/2023/03/D2.1_EndUserNeedsKPIs_PU.pdf
2. D2.2 | Architecture specification. www.heron-h2020.eu/wp-content/uploads/2023/03/D2.2_ArchitectureSpecification_CO_Redacted.pdf
3. ENGAGE IMS/CAD. satways.net/products-sw/engage-ims-cad/

PLOTO

PLOTO: Improved IWW resilience using predictive modelling, environmentally sustainable and emerging digital technologies and tools

Dimitris Liparas[1], Dimitrios Vamvatsikos[2], Nikos Avgerinos[3*], Anna Zanetti[4], Alexios Pagkozidis[5], Didier Bousmar[6], Natalia Budescu[7], Erzsébet Szabó-Aranyi[8], Alexis Melitsiotis[9], Themis Vokali[10], Vasileios Melissianos[11], Fotios Barmpas[12]

1. Research and Innovation Development, Netcompany-Intrasoft S.A.
2. School of Civil Engineering, National Technical University of Athens
3. Diadikasia Business Consulting S.A.
4. ERTICO – ITS Europe
5. Satways Ltd.
6. Direction des Recherches hydrauliques, Service public de Wallonie
7. Asociatia Romanian River Transport Cluster
8. Budapesti Szabadkikoto Logisztikai Zrt.
9. EXUS AI Labs
10. RISA Sicherheitsanalysen GmbH
11. Societal Resilience and Climate Change Center of Excellence
12. School of Mechanical Engineering, Aristotle University of Thessaloniki

INTRODUCTION

The annual World Bank International Logistics Performance Index ranks no less than 13 European economies in the top 20 of global leaders in logistics.1 Global freight traffic is anticipated to triple for inland modes in the next 30 years.2 In addition, in the EU, surface freight traffic is expected to rise by 53% by 2050.3 In spite of these projections, the growth of the sector is not without complications. The biggest concern is how economic gains from increased demand can be sustained when considering adverse externalities and possible rebound effects. Digitalisation and increased automation have the potential to reduce administrative burdens, lower operational barriers and so improve efficiency, productivity, interoperability of processes and competitiveness4 in the multimodal freight transport nodes.

The EU-funded project PLOTO platform aims to address multi-hazard risk understanding, smart prevention and preparedness, as well as faster, adapted and efficient response proposing a new integrated system to support operational and strategic adaptation and mitigation measures. It achieves its stated goals by better absorbing and efficiently recovering from Climate Change impacts, including extreme events, thus increasing the resilience of Inland WaterWays (IWW).

METHODOLOGY

PLOTO is a pure technological project, but it is driven by the actual needs of the end-users, mainly IWW operators, including inland ports, authorities, and shipping companies. The pilot activities scheduled within the project life-time have as ultimate goal the achievement of a minimum TRL7 concerning the technology components and the overall system developed in its context. PLOTO will follow a process of iterating a series of activities, performing preliminary module and system assessments and validation campaigns well before the pilot demonstrations.

The technological backbone of PLOTO includes Climate, Atmospheric Forcing, and Multi-Hazard Modelling, Multi-Hazard Vulnerability Modules and Assessment Toolkit (MHVAT) for IWW and assets, Improved Computer Vision (CV) Techniques and ML Techniques, Remote Sensing, including Quick Assessment Damage Maps, Fore-Now/Casting Weather Predictions Methods & Tools, PLOTO Middleware and Data Fusion (DF), IWW Assessment Tool (IWAT) and IWW Digital Twin (DT), Enhanced visualisation Common Operational Picture, Incident Management System, and Decision Support System. At its basis, a modular design is adopted to connect hazards, exposed assets and interconnected infrastructure networks to form a digital twin of the IWW that interacts with all PLOTO modules to efficiently transfer and process sensor data (Figure 1).

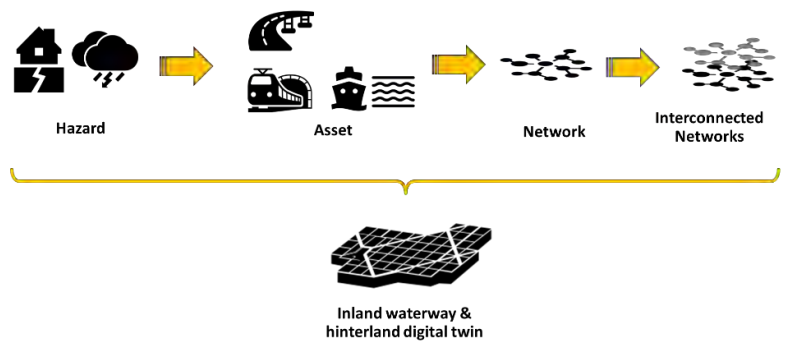


Figure 1. *The proposed digital twin formulation that forms the core of PLOTO*

Use cases and scenarios

Three project pilot sites in Belgium, Hungary and Romania will be the testbeds to demonstrate the suitability of the PLOTO platform focusing on the following main objectives: 1) to improve multiple-hazard assessment and strategic management for protection of hotspots of the IWW ports and sections, 2) to improve strategic and operational decision making, 3) to test the various PLOTO outcomes and the overall integrated DSS tool with actuation technologies in real-scale critical parts of the IWW. The Danube area in Romania, the Budapest inland port in Hungary and the Belgian region of Wallonia have been selected because of the specificities of the territory and the different impacts of extreme environmental conditions in the selected portion of IWW.

Acknowledgements

This work is a part of the PLOTO project. This project has received funding from the Horizon Europe innovation actions under grant agreement no. 101069941.

References

1. World Bank (2018). Connecting to Compete - 2018 Trade Logistics in the Global Economy: The Logistics Performance Index and Its Indicators, p. 12.
2. OECD - International Transport Forum. (2019). ITF Transport Outlook 2019, p. 39.
3. European Commission. (2018). In-depth analysis in support of Commission Communication COM(2018) 773 - 'A Clean Planet for all: A European long-term strategic vision for a prosperous, modern, competitive and climate neutral economy', p. 82.
4. European Commission. (2018). State of play and barriers to the use of electronic transport documents for freight transport Options for EU level policy interventions: final report - Study, pp. 19-20.

PRAETORIAN

PRAETORIAN: From protection to resilience of critical infrastructures

Eva Muñoz-Navarro[1], Juan José Hernández-Montesinos[1], Antonio Marqués-Moreno[1], Lazaros Papadopoulos[2], Antonios Karteris[2], Konstantinos Demestichas[2]

1. ETRA Investigación y Desarrollo
2. School of Electrical and Computer Engineering, National Technical University of Athens

1. Regulation and the PRAETORIAN solution: an overview

The new CER Directive [1] constitutes a considerable change as compared to the ECI Directive 2008/114/EC [2], since critical entities will have to meet specific obligations aimed at enhancing their resilience. Moreover, a wider sectoral scope will allow Member States and critical entities to better address interdependencies and potential cascading effects of an incident. European critical entities are more interconnected and interdependent, which makes them stronger and more efficient but also more vulnerable in case of an incident.

As requested by the CER Directive, critical entities will need to carry out risk assessments on their own, take technical and organisational measures to enhance their resilience and notify incidents. New tools will soon be demanded by CI operators and innovative technologies will have to be used allowing the adoption of these measures. The CER directive is complemented by the NIS2 Directive [3], thus becoming an updated and comprehensive legal framework to strengthen both the physical and cyber-resilience of critical infrastructure.

The goal of the H2020 PRAETORIAN project (https://praetorian-h2020.eu/) is to enable the security stakeholders of the CIs in Europe to manage the lifecycle of security threats, from forecast, assessment and prevention to detection, response and mitigation, in a collaborative manner with the security teams from related Cis, being the CIs in the same sector or not. PRAETORIAN proposes a toolset that:

a) makes use of data obtained from relevant legacy security systems of the CIs,

b) introduces novel sensors and innovative data analysis,
c) builds a model of the ecosystem of CIs,
d) improves the channels and quality of communication among stakeholders,
e) combines the emergency plans of those CIs.
The combination of these functionalities will support the decision-making process of CI operators to prevent major damages to the installations, neighboring population and the environment, while allowing a fast recovery after incidents.
The PRAETORIAN toolset consists of four innovative products, which intend to provide the security managers with the capacity to protect the CIs from physical, cyber and combined (physical and cyber) attacks. The Cyber Situation Awareness (CSA) system can recognize patterns within the network and generate corresponding events. The Physical Situation Awareness (PSA) system can be integrated with existing sensors and legacy systems in the CI to collect meaningful data and combine them with information received from newly developed modules that implement drone detection and video analytics. Both the CSA and the PSA generate an alarm when cyber/physical threats are detected. The Hybrid Situation Awareness (HSA) system uses a digital twin of the related CIs to correlate the received alarms and estimate the cascading effects on own and related CIs. This information is processed in the Coordinated Response (CR) system which suggests an effective response to the threat, allowing notifications and information sharing through multiple channels.

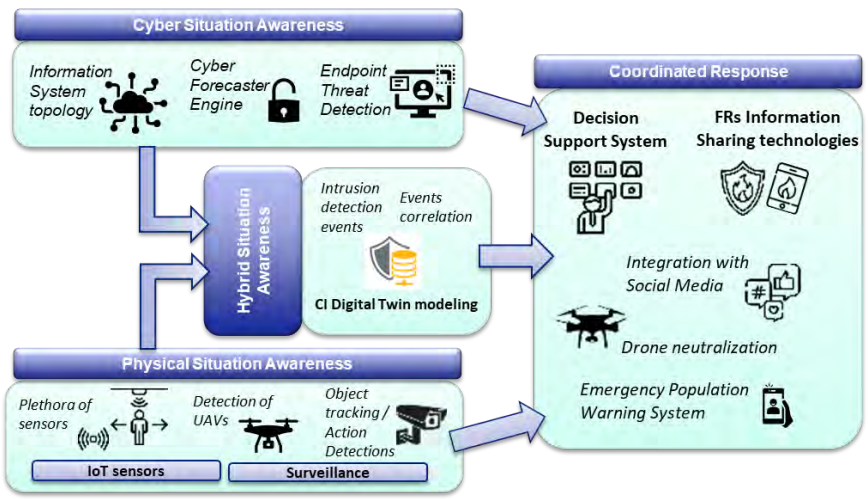


Figure 1. *PRAETORIAN Platform*

PRAETORIAN focuses on interoperability of CIs legacy systems together with new novel systems and sensors, aiming at improving the capability of CI security managers to prepare and apply in practice the Resilience Plan as requested by the CER Directive. This means to take technical, security and organisational measures. Moreover, PRAETORIAN also allows the integration of additional information sources, such as signals from social media, agencies or any other open sources. Social media is indeed a valuable source of information during emergency situations, since it can be used to further improve the situation awareness of First Responders and rescue teams so they are able to act more effectively [4].

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021274. 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. DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive)
2. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
4. A Methodology for enhancing Emergency Situational Awareness through Social Media. ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security. August 2022. Article No.: 130. Pages 1–7.

PRECINCT

PRECINCT

Security challenges in critical infrastructures in transport: the PRECINCT Athens use case

Ioannis Lymaxis[1], Eftichia Georgiou[2]

1. Inlecom Innovation
2. Center for Security Studies

Abstract: The interrelationships between critical infrastructures (CIs) have become more complex, rendering the security and resilience management of cyber-physical attacks and natural hazard threats more challenging. The EU-funded PRECINCT project connects private and public CI stakeholders in a geographical area to a cyber-physical security management method that will produce a protected territory for citizens and CIs. The project delivers a framework specification for systematic CI security and resilience management, a cross-facility collaborative management infrastructure enabling stakeholder communities to create PRECINCT ecosystems and increased resilience support services, a vulnerability assessment tool using serious games, PRECINCT's Digital Twins, and PRECINCT Ecosystems in four large-scale living labs and transferability validation demonstrators.

1. Introduction

EU Critical Infrastructures (CIs) are becoming more and more vulnerable to physical and cyber-attacks as well as natural disasters. The focus of research and newly developed solutions is on the protection of individual CIs, however as most of the CI interrelationships have grown more intricate and rely on interconnected networks and devices, the failures in a critical sector may result in cross-sector -or even cross-border- cascading effects. The lack of proper awareness makes it difficult for operators to anticipate risks, protect the CI's critical services and enable rapid recovery in the event of disruptions.

Through the application of PRECINCT project methodological framework and technological solutions developed, the work presented in this paper concentrates on improving the phases of crisis management that deal with the preparedness and response capabilities of interconnected CI's operating in the same geographical area. In this regard, three main tools, namely LL3 Digital Twin and it's components, the Serious Game and the Coordination Center for providing a common situational awareness picture to all relevant stakeholders involved during a crisis are described. The findings and developments presented, are linked with the EU funded project PRECINCT aiming to link private and public CI stakeholders in a geographic area to a common cyber-physical security management approach that will result in a protected area for people and infrastructure.

2. Methodology

PRECINCT (1) will develop a comprehensive Ecosystem Platform, connecting various stakeholders of interdependent CIs and Emergency Services, enabling them to collaboratively manage security challenges and enhancing their resilience against hybrid attacks. The overall goal is to provide new services and capabilities to CI operators, utilizing Artificial Intelligence (AI) and Machine Learning (ML) techniques, for early detecting and managing cyber-physical threats, thus strengthening CI defenses against vulnerabilities.

The following are the areas in which the project's research has been conducted along this line:

Understanding: PRECINCT uses State of the Art (SOTA) modelling techniques to precisely determine the present and future risks in territory-based interdependent CIs under various multi-hazard conditions and configurations, to gain a deeper understanding of interdependent CIs. A key goal is to enable CI actors to anticipate sophisticated attacks, to detect anomalies and to incentivize optimized command structures and coordinated responses between CIs and first responders, thereby minimizing cascading effects and allowing rapid recovery.

Improving: The Digital Twins will help improve accuracy and automation in identification, remediation, and threat elimination. The application of Digital Twins to multi-hazard risk management yields a circular process of anticipating, preventing, and protecting events, responding during the events, and recovering and learning after events.

Sustaining: Modelling CI interdependencies to identify, forecast or simulate potential cascading effects has limitations in identifying vulnerabilities in complex

and co-dependent CI threat contexts. The dynamic nature of the threat canvas reshapes based on new weekly exploits, the ingenuity of attackers in finding new and creative angles of attack, thus static and dynamic modelling approaches require considerable time and effort to maintain.

By the end of the project, through a series of validation scenarios demonstrated in four Living Labs (LL), the project will produce tools that are ready for use. The current paper will mainly focus on the demonstrations of the Athens LL, involving several operators, i.e. the Athens International Airport, the Attikes Diadromes S.A., and the Attiko Metro S.A., having as an end goal to increase the involved CIs overall resilience against cyber-physical incidents affecting urban transport. Since the Athens LL participants represent the city's main transportation system (the rail and road network along the Athens Airport / Attiki Odos corridor as well as along the urban rail and road network), with a population of over 4 million and which is typically visited by more than 25 million people annually, the demonstration represents a difficult but essential case for resilience management of interconnected transportation systems as well as for demonstrating the efficiency and importance of PRECINCT tools.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021668. 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. PRECINCT. [Online] https://www.precinct.info/en/about/.
2 PRECINCT Grant Agreement (Grant agreement ID: 101021668)
3. PRECINCT D1.2 Critical Infrastructure Interdependencies and Cascading Effects interdependency Graphs\
4. PRECINCT D1.3 Resilience Methodological Framework
5. PRECINCT D5.5 LL3 Operation Athens

METICOS

METICOS

Best Practices for Creating and Maintaining Clusters in EU-Funded Projects Insights from the H2020 BES Cluster

Charalampos Chatzimallis[1], Danai Kyrkou[1], Anneta Kampouridou[1], Christiana Themistocleous[4], Alkiviadis Astyakopoulos[3], Artemisia Nikolaidou[3], Mirela Rosgova[3], Sule Yildirim[2], Pantelis Velanas[4]

1. ViLabs OE
2. Norwegian University of Science and Technology
3. Center for Security Studies (KEMEA)
4. European University of Cyprus

Abstract

EU-funded projects often use clustering or sister-project communities as a dissemination and communication strategy to promote their outputs and exchange knowledge. However, it can be challenging to maintain such communities and have a meaningful impact on projects' life during or after the funding period. This paper aims to provide answers and best practices to questions related to creating, managing, and maintaining clusters, engaging projects, ensuring sustainability, and supporting efficient joint exploitation activities. Focusing on the latter, it draws insights from the H2020 BES Cluster (H2020 Border External Security Cluster), which consists of security-related H2020 and Horizon Europe projects collaborating to support communication and dissemination activities, exchange good practices and methodologies, and explore possibilities to combine pilot activities. The paper provides a comprehensive review of the outcomes and impact of the H2020 BES Cluster projects, highlighting their significance and potential for further exploitation. Moreover, it discusses strategies for early exploitation and effective dissemination for projects still in progress. Although the H2020 BES Cluster is border security-related, its proposed methodology and practices can apply to different projects with minor customisation. This paper aspires to introduce and strengthen innovations and improvements to the security and border control system within the EU by promoting a collaborative environment and drawing attention to the tangible results and benefits of EU-funded projects.

Introduction

In EU-funded projects, clustering is crucial in enabling collaboration and innovation among different stakeholders in a particular industry or field. This paper, drawing on insights from the H2020 BES Cluster, reviews the outcomes, impact, and potential for further exploitation of the projects within the cluster. This paper aims to promote collaboration and draw attention to the tangible results and benefits of EU-funded projects, introducing and strengthening innovations and improvements to the security and border control system within the EU. Integrating clustering in EU projects' plans fosters knowledge exchange and the development of sustainable products and services (Delgado et al., 2014).

Methodology

Building a cluster is like building a community. The BES Cluster reviewed a number of community-building methodologies and best practices, drawing inspiration from the European Commission's "Communities of Practice Playbook" and Wenger-Trayner's "Introduction to Communities of Practice" to finally structure its own, customised approach. The BES Cluster set 7 steps to follow, towards building its community of projects: Identify the target audience: Research and understand the needs, interests, and goals of stakeholders in the security sector consortia. Develop a mission and values statement: Create a guiding statement reflecting the community's purpose and goals. Create a communication plan: Outline channels, and frequency of communication, including social media, events, and a mailing list.
Establish a leadership team: Set a diverse leadership team that can work together to achieve the community's goals. Encourage participation: Promote engagement in Cluster activities like workshops, events, and panels. Foster a culture of inclusivity: Create a welcoming and supportive environment by actively promoting diversity, equity, and respect. Evaluate and adapt: Assess the effectiveness of community-building process, considering its impact and make adjustments as needed.

Case study: Meeting the BES Cluster

The BES Cluster was created in 2020 by the METICOS project to promote interactions among similar projects (FP7, H2020, Horizon Europe) and other stakeholders

like policymakers, industry and academia to promote knowledge exchange. The projects collaborate to identify solutions to upcoming challenges, secure effective dissemination and valuable exploitation potentials, and generate knowledge that will change the current state-of-the-art in their fields.

In the last three years of the existence of the BES Cluster, several joint dissemination and piloting activities have taken place. One notable accomplishment is the demonstration activities at Piraeus Cruise Port organised by the TRESSPASS Project, with METICOS representatives participating as observers. This success story highlights the power of knowledge exchange within the H2020 BES Cluster.

Additionally, the 1st PROMENADE Workshop organised in December 2021 has been supported by the BES Cluster and broadly disseminated through its network and communication channels. The event was attended by 88 participants from 12 European countries, including FRONTEX, EU organisations, large industries, SMEs, RTOs, academia and others. After the Workshop, a database was created to keep traceability of engaged stakeholders and establish communication channels for future project activities and trials.

Furthermore, the H2020 BES Cluster actively participated in two NESTOR Workshops. The 1st one which was related to the Roadmap for Border Management Standardisation took place at the CCMC in Brussels in cooperation with the CEN-CENELEC Sector Forum on SecurityBrussels, on 17 February 2023. The full-day workshop had a total of 85 onsite and online participants. The 2nd NESTOR Workshop, namely Demo Day & Final Workshop was held on 24 April 2023 in Athens. It was a full-day hybrid event demonstrating the operational capabilities of the NESTOR platform, as they were developed and tested throughout the land & maritime trials in Lithuania, Cyprus and Greece. More than 190 attendees participated having the opportunity to see the NESTOR project achievements, the Trials' demonstration through six dedicated videos and the live presentation of all NESTOR project assets, including the BC3i platform, surveillance cameras, mixed reality HoloLens glasses, RF sensors and unmanned vehicles (tethered drones, autonomous ground vehicle and underwater vehicle.

Currently, the Cluster counts 17 EU-funded project members, 287 partners from 37 countries, and more than 45 piloting activities. The projects are creating different border management tools however, many of them are versatile and can be adapted to other industries, such as IT, education, health, energy and logistics.

Conclusion: The future of the BES Cluster

Many BES Cluster members are approaching completion, and they aspire to keep the BES Cluster alive and use it as an exploitation tool for their results. This can be facilitated by creating a BES library to store research papers, technical reports, case studies, best practices, and policy documents related to border external security.

Another way to continue boosting the sustainability of the Cluster is to promote joint communication, dissemination and exploitation activities (European Commission et al., 2019). METICOS is planning to showcase its successful testing and the Social Sensing toolkit, inviting end users of BES Cluster projects. Additionally, the BES Cluster is exploring collaboration opportunities with partners from BES projects at the Ninth Italian Conference on Computational Linguistics (CLiC-it 2023).

This paper provides insights into the importance of clustering activities in EU-funded projects. However, additional topics and information couldn't be included due to the word limit. These topics will be further explored and expanded upon in the final paper.

Acknowledgement

These projects have received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreements No. 883075, 101021851 and 101021673.

References

1. Delgado, M., Porter, M. E., & Stern, S. (2014). Clusters, convergence, and economic performance. Research policy, 43(10), 1785-1799.
2. European Commission, Executive Agency for Small and Medium-sized Enterprises, Haardt, J., Weiler, N., Scherer, J., et al. (2019). Making the most of your H2020 project – Boosting the impact of your project through effective communication, dissemination and exploitation. Retrieved from https://data.europa.eu/doi/10.2826/045684
3. European Commission. (n.d.). Communities of practice playbook: Methodology. Retrieved from https://bit.ly/3pPxBm1
4. Wenger-Trayner, E. and Wenger-Trayner, B. (2015) An introduction to communities of practice: a brief overview of the concept and its uses. Retrieved from https://bit.ly/3pPxBm1

BorderUAS

BorderUAS Project

Dimitrios Myttas[1], Elisabeth Bellou[1], Agathi Barbaki[1], Eirini Papadopoulou[1], Ioannis Evangelopoulos[1], Theodoros Katsilieris[1], Ioannis Athanasakis[1]

1. KEMEA (Center for Security Studies)

BorderUAS brings together a total of seventeen (17) organizations with the aim of bringing off a border and external security enhancing technological project. The BorderUAS project pioneers in featuring a lighter-than-air (LTA) unmanned aerial vehicle (UAV) equipped with an ultra-high resolution multi-sensor surveillance payload serving the trifold scope of border surveillance (relevant to transnational organized crime activities), search and rescue (SaR) activities as well as that of rough terrain detection.

In particular, the sensor/camera payload will come equipped with a synthetic aperture radar (SAR), a shortwave/longwave infrared (SWIR/LWIR) & acoustic cameras meant for landscape mapping, coupled with optical & hyperspectral cameras intended for indirect detection (by means of vegetation disturbance). BorderUAS is further capitalizing on participating border police infrastructure (command & control centers), innovative data models (for irregular crossing patterns & preferred migratory routes identification) & advanced audio/video analytics & storage (for adding to the UAV's detection capabilities) to achieve its declared set of goals.

Innovative technological features incorporated into BorderUAS will be showcased, in near real-life conditions, through a series of three (3) field-trials taking place in locales along the three (3) major irregular migration routes (i.e. Eastern Mediterranean, Western Balkans & Eastern Border Routes) accounting for up to 58% of all irregular border crossing detections. BorderUAS Consortium Members cover a wide variety of subject-matter expertise, ranging from technical facets (Technical Partners) to border surveillance policing (Greece, Bulgaria, Romania, Moldova, Ukraine) and the ethical-privacy/human right protection spectrum (NGOs, regulatory experts etc.).

The three (3) above-mentioned field-trials, seeking to enhance interagency collaboration synergies among the five (5) law enforcement agencies (Greece, Bulgaria, Romania, Moldova, Ukraine) partaking to BorderUAS, will be carried out in the below-listed destinations:

- Near HSF Partners' HQ in Croatia,
- With proximity to Romanian borderlands, listing the participation of Romanian & Moldovan Border police units,
- With proximity to Hellenic-Bulgarian borderlands, featuring a synergy between Hellenic & Bulgarian Border police forces.

Upon the project's conclusion, experience gathered from all three (3) field-trials will be processed into a compiled report delineating system performance & lessons learned from diversified weather & terrain experimentation.

Overall, BorderUAS is expected to provide a high coverage, resolution & revisit time low-cost solution (4 EUR/kg/hr) as opposed to satellites, while featuring higher endurance (100 kg payload for 12h) than drones. The conceptualized technological innovation will be further featuring in border surveillance management & market integration once the BorderUAS Project reaches its conclusion.

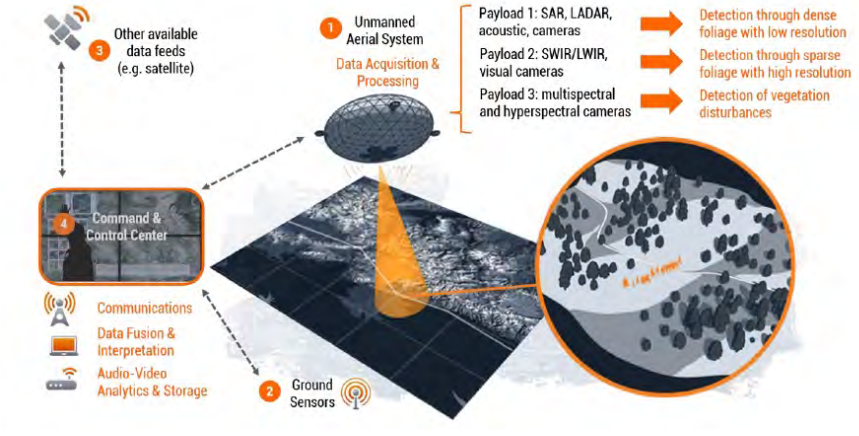


Fig. 1. *Innovative technological elements of the solution combining aerial and ground sensor data acquisition, processing, fusion, interpretation, analytics and storage.*

In a nutshell, BorderUAS has set forth the following objectives that it seeks to achieve:
• the enhancement of interagency synergies between different border police jurisdictions.
• The innovative & versatile merging of several different sensor & camera components to allow for optimized border surveillance & through foliage penetration solutions.
• The employment of state-of-the-art Machine Learning data models to provide end-users with more articulated options as concerns the storage, modification & analysis of UAV payload feed while on target detection.

Acknowledgements
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883272. 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.

EURMARS

EURMARS An advanced surveillance platform to improve the EURopean Multi Authority BordeR Security efficiency and cooperation

Kriechbaum-Zabini Andreas[1]

1. Austrian Institute of Technology

1. Challenges and objectives
European maritime border management is a complex and multifaceted task. The EURMARS project addresses the main challenge of irregular migration attempts, smuggling, and trafficking, along with the management of search and rescue operations, oil spill observation and monitoring, in addition to addressing the coordination and cooperation among different authorities and agencies at the national and EU level. The EURMARS project aims to improve border surveillance systems in Europe through the development, deployment, and validation of a 24/7 surveillance platform with the following characteristics: (i) provision for integration of existing and future data sources and services; (ii) utilisation and clustering of high-altitude technology, satellite imagery, UAVs, and ground-based sensors into a joint surveillance capability to provide continuous complementary data; (iii) innovative coupling of sensors data with data fusion, AI analytics, risk assessment, and alarming functionality; (iv) flexible interoperable surveillance platform with multi-authority cooperation capabilities and verified easy-to-integrate potential for next generation platforms and systems; (v) performance benchmark platform to ensure acceptability by all stakeholders including extensive technical and user acceptance tests and ethical and legal impact assessments.

2. Concept and approach
The EURMARS project will enhance EU efforts in addressing increasingly complex security risks and threats regarding border management in the maritime domain

by designing and implementing a multi-authority border surveillance platform that integrates AI, risk assessment and visualisation innovations supported by advanced sensing technologies, such as high altitude platform systems, satellite imagery, unmanned vehicles (UxVs) and ground-based sensors. The EURMARS platform will improve both situational awareness and operational efficiency for a wide range of maritime security risks and threats and will be evaluated for its viability and effectiveness in the following Pilot Use Cases: (1) PUC1 - Maritime Border Control: Detection of trafficking and other illegal activities, (2a) PUC2(a) - Search & Rescue, (2b) PUC2(b) - Maritime structures and oil spills surveillance & monitoring; and (3) PUC3 - Land border control; illegal crossing outside of business contingency plans.

3. Expected results and targeted end-users

The main expected result is the EURMARS integrated system achieving significant performance enhancements in terms of endurance, reliability, permanence and coverage over existing surveillance assets. Intermediate results include the analysis and description of a comprehensive set of validated and prioritised stakeholder requirements supporting use case technical development, validation and user acceptance, the EURMARS secure interoperable architecture and the EURMARS components/subsystems enabling the 24/7 EURMARS surveillance platform supporting advanced functions of data analytics, risk assessment/ alarming and visualizations (All components and overall integrated system expected to achieve TRL 7 at the end of the project). The operational validation in real life scenarios and three Pilot Use Cases of the EURMARS platform blueprint, an AI Foresight Report and Blueprint containing PIA, EIA and SIA assessments and best effort attempt to create open-source domain-specific benchmark datasets and contribution to relevant international standards comprise the additional expected results.
The main end users to benefit from the project results are authorities and agencies at the national and EU level, such as coast guards, border guards, customs, police, fisheries, environmental protection and maritime safety entities.

Acknowledgements

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073985. This article reflects only the authors' views and both the Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains.

FLEXI-Cross

Flexible and Improved Border-Crossing Experience for Passengers and Authorities

Giuseppe Vella[1], Thomas Azrak[2], George Tournakis[3]

1. Engineering Ingegneria Informatica S.p.A
2. EBOS Technologies Limited
3. Hellenic Police

1. Background

1.1 The FLEXI-cross challenges

Freight and passenger transport is an ever increasing and significant part of the European Economy. EU transport exports experienced an increase of 9% totalling at €66 billion in 2018, while the total exports and imports of EU have reached €5.9 trillion and €6 trillion respectively [1]. International, multimodal freight transport is steadily in- creasing in the EU-27 [2]. The increasing importance of pan-European passenger and freight transport, both in terms of financial as well as societal impact, is showcased by the adoption of the EU vision of Trans-European Transport Network (TEN-T) [3], which will connect and enhance trade and tourism among European nations as well as between EU nations and neighbouring countries. Such enhanced mobility will intensify border-crossings of citizens and goods, which in turn will generate a significantly increased load on customs and security procedures, calling for smarter, more effective and cost-efficient solutions for border checks.
On the other hand human trafficking, irregular crossings and contraband smuggling is going to become a major concern for EU.
The need for increased security, privacy and protection at EU borders becomes even more critical under such circumstances. The increased load and importance of passenger and freight border-crossings calls for even more flexible, dynamic and effective procedures when it comes to border-checks, which can be enabled by innovative technologies, such as 5G and Internet of Things (IoT), Artificial Intelligence

(AI) and Machine Learning (ML), Big Data and Predictive Analytics, Cloud and Edge Computing and more.

1.1 The FLEXI-cross approach

The FLEXI-cross solution is developing and will deploy as an innovative border-checking solution, in real operational environments, addressing road, rail and port borders. The resulting flexibility and dynamicity of border check planning will offer novel capabilities such as dynamic deployment of check-points and support via mobile applications for border personnel, while guaranteeing high level of security, privacy of personal data and protection of people's fundamental rights. The unique value proposition of FLEXI-cross are the following:

Predictive Risk Assessment of vehicles and people based on distributed data and camera feed processing, enabling abnormal behaviour detection and providing anti-trafficking and anti-smuggling protection.

Enhanced border security through portable biometric based checks (fingerprint, facial recognition), enabling quick and secure person verification and allowing for real-time cross-referencing with other data sources / databases.

Flexible, fast and cost-effective deployment of ad-hoc Border Check Points (BCPs), with the use of mobile / portable solutions and equipment.

Secure, private and traceable sensitive / personal data exchange based on the FLEXI-cross blockchain, enabled data change and processing framework.

More (time and cost) efficient border checking procedures at EU borders through optimisation (flow management, active planning) based on real-time data, historical data, available resources and traffic estimations.

Increased safety and improved experience for border-personnel based on advanced Human Machine Interfaces (HMIs) for immediate feedback and enhanced situational awareness via Augmented Reality (AR) devices.

The FLEXI-cross project will instantiate three different use cases addressing road, port and rail-based border-crossing conditions in three different sites, namely the Danube based port of Galati in Romania, the Greek-Bulgarian borders at Ormenio and the Romanian-Moldovan rail crossing.

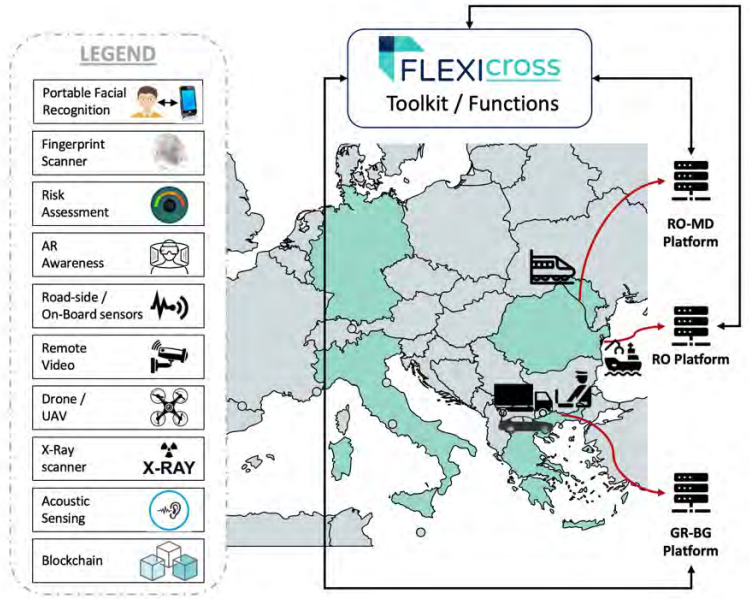


Figure 1. *Pilots location and technologies used*

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101073879. 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. World Trade Statistical Report 2019, https://www.wto.org/english/res_e/statis_e/wts2019_e/wts2019_e.pdf
2. Freight transport statistics, Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Freight_transport_statis-_tics&oldid=492516#Road_transport
3. Trans-European Transport Network (TEN-T) core corridors: http://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/map/maps.html

FOLDOUT

Through-foliage detection, including in the outermost regions of the EU

Kriechbaum-Zabini Andreas[1]

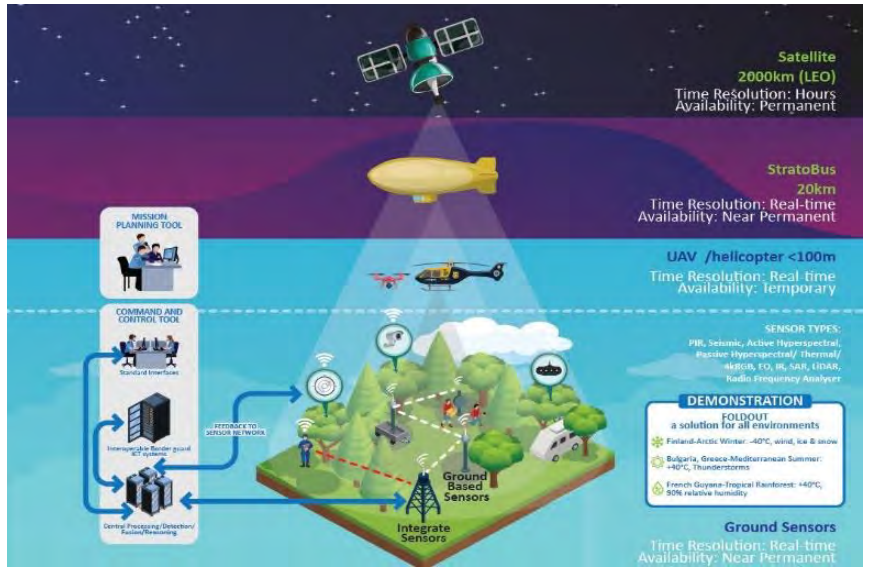
1. Austrian Institute of Technology

OBJECTIVES

The FOLDOUT platform assists border guards by providing prompt detection of illegal activity at borders and trace the movement and routes prior to arrival in border areas. FOLDOUT builds a system that combines various sensors and technologies and intelligently fuses these into an effective and robust intelligent detection platform. FOLDOUT makes the tasks of Border Guards simpler and faster by combining events from various sensors to give a complete situation threat assessment combined with suggested reaction scenarios.
With a two-year pilot in Bulgaria and demonstrators in Greece, Finland and French Guiana, FOLDOUT has demonstarted fundamental enhancements in the domain of border surveillance and improved search & rescue scenarios.

DESCRIPTION

The technical concept of FOLDOUT is based on the combination of several sensor technologies on the ground and on special, high rising platforms with data fusion algorithms into a single, seamlessly integrated system. This concept allows for the real-time detection of critical events (e.g. illegal cross border activities, lost persons) even under dense foliage. The alarms are presented to border guard operators in a common operational picture in a unified data presentation for all sensors.
To penetrate the foliage to a certain extend under day and night conditions long range, multi-spectral, LIDAR and RADAR sensors are used. For the surveillance of large border areas stratospheric platforms are employed to yield unobstructed field-of-view and unprecedented detection range for the sensors they carry. Ground EM (radio transmitter detection), acoustic and seismic (movement) detectors deliver complementary data where the vegetation is too dense to penetrate. The activities at the fringe of the foliage, such as suspicious car traffic, are monitored by conventional ground-based cameras and EOS sensors completed by satellite SAR data.
All the different sensors are integrated in a common system and data model to provide information on different aspects and in a different light spectrum or modality or even on a different time resolution or scale. Data processing algorithms based on machine learning therefore is used to fuse and reliably interpret all data to derive alarms on the presence of persons or critical situations in the surveilled area. Reasoning methods are used to filter unusual from usual behavior in the surveillance area. To reduce operator workload and improve situational awareness sensor information and alarms are uniformly presented to the operator on a command-and-control software tool. The tool provides a map-based graphic user interface with a standardized symbology to observe, track and react with maximum efficiency.



RESULTS

The main result of FOLDOUT has been a demonstrated system and solution to detect and locate people and vehicles operating under the coverage of trees and other foliage over large areas. FOLDOUTs further results are:
• Developed requirements closely together with the end users, e.g. border guards;

• Improved sensor technologies with innovative approaches specifically adapted to through foliage detection scenarios, functioning at day as well as nighttime and in harsh environment;
• Improved situational awareness through fusion of advanced aerial and space-based sensor platforms with ground-based sensors into one surveillance solution;
• Demonstrated effectiveness of the FOLDOUT concept in realistic operational scenarios;
• Provided a planning tool for decision makers to configure a surveillance system for the specific requirements of a target deployment area;
• Created a scientific/industrial development community and putting at their disposal a set of reference data, which will be used to tune and assess the analytics performance.

Melchior

MELCHIOR

Non-contact technologies for fast detection of threats on individuals: the vision of MELCHIOR project

Michael Ellis[1], Juha Hintsa[1], Valentina Scioneri[1], Toni Männistö[1], Mirela Rosgova[2], Eirini Papadopoulou[2]

1. Cross-border Research Association (CBRA)
2. Center for Security Studies (KEMEA)

1. MELCHIOR challenge

For decades, law enforcement and security professionals have been well aware of the threat posed by individuals carrying weapons, explosives, or drugs at public events, border crossings, and prisons. However, the nature of the threat has evolved dramatically in recent times, with dangerous articles now being concealed not only on the body or in clothing, but also inside body cavities. This includes concealment not only inside natural human body cavities, but also evidence of "terror doctors" who conduct operations to implant devices or articles inside suicide bombers. These devices can be concealed in body fat, around the chest, shoulders, breasts, buttocks, and other body parts. As a result, it is crucial for security professionals to stay up-to-date with evolving threats and technology to detect such concealed items and prevent potential attacks.

2. MELCHIOR goals

The MELCHIOR project is focused on improving the detection of illicit goods such as drugs, explosives, and weapons, concealed on individuals and in critical body cavities using non-contact detection technologies. The project aims to develop blast-proof prototypes of inspection stations that have improved sensitivity and detection capabilities, extending to limbs and body cavities.
The main benefit of the MELCHIOR technologies are that they increase the safety of

border and security staff as they do not have to touch inspected individuals, while also improving the comfort of travelers, sports fans, inmates and prison visitors as there is no undressing or patting by hands required.

MELCHIOR develops a range of advanced technologies to detect and respond to various threats (see the figure below). These technologies include an infrasound generator, which can detect low-frequency sound waves. The project also uses a vibroacoustic model to analyze sound wave interactions with threat materials. Point millimeter wave reflection and point THZ wave reflection technologies are used to scan for hidden objects or materials in sensitive, hard-to-reach places such as body cavities. Broad-range velocity sensors are employed to detect movement and other physical changes during the inspection. An acoustic tuned blast-proof cabin provides a safe environment for security staff and bystanders. Fast cabin disinfection helps to prevent the spread of pathogens, while the trace detection of chemical and biological aerosol samples helps to identify hazardous materials. Artificial intelligence is also used to analyze data and identify potential threats, making the MELCHIOR project a cutting-edge example of how technology can be used to enhance security and safety.

3. MELCHIOR use cases

As part of the project's demonstration phase, prototypes of the MELCHIOR technologies will be showcased in different operational environments. In Spain, the prototype will be installed at the Madrid-Barajas airport and a port, where tests will be conducted and workshops and system demonstrations will be given to Spanish security authorities. The Spanish Prison Services is also prepared to demonstrate MELCHIOR prototypes at their facilities. In Romania, the prototype will be installed at the Giurgiu Border Crossing Point in Giurgiu County to test and compare its effectiveness with existing technologies. The Hellenic Police will participate in a demonstration event at a Greek-Turkish border "Point of entrance". Finally, a prototype will be installed at a sports arena in Finland to demonstrate capabilities of MELCHIOR innovations in large events at a stadium.

Acknowledgements

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101073899. This article reflects only the authors' views. The Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains.

NESTOR

"NESTOR: Next-Generation Holistic Border Surveillance System for Effective Pre-Frontier Situational Awareness and Enhanced Border Control Measures in the European Community"

Mirela Rosgova[1], Efstathios Skarlatos[2]

1. Center for Security Studies (KEMEA)
2. Center for Security Studies (KEMEA)

Introduction

The European Community has faced various challenges in recent years due to the increase in irregular migration flows and transnational crimes, particularly smuggling activity in the Eastern EU Borders. This has led to the need for a next-generation holistic border surveillance system that provides pre-frontier situational awareness to assist the relevant authorities in making more informed decisions about border control and response operations. NESTOR aims to address these challenges by demonstrating a fully functional border surveillance system.

Objectives and Methodology

NESTOR's objective is to develop a next-generation holistic border surveillance system that will provide long-range and wide area surveillance capabilities for detection, recognition, classification, and tracking of moving targets, based on optical, thermal imaging, and Radio Frequency (RF) spectrum analysis technologies. This achieved by creating an interoperable sensor network, including stationary installations and mobile manned or unmanned vehicles (aerial, ground, water, underwater) capable of functioning both as standalone, tethered, and in swarms. Furthermore, NESTOR's system fuses in real-time border surveillance data combined with web and social media information, creating and sharing a pre-frontier intelligent picture to local, regional, and national command centers in AR environment being interoperable with CISE and EUROSUR.

Desk Research and Technical Solutions

NESTOR's system provides a significant advantage over existing border surveillance systems as it has a more extensive range of surveillance capabilities, including the ability to detect, track, and classify moving targets in areas that are typically difficult to monitor due to geographical constraints. Additionally, the system's fusion with real-time web and social media information is creating a more comprehensive and intelligent pre-frontier picture, which assists the relevant authorities in making more informed decisions about border control and response operations. Furthermore, the interoperability of NESTOR's system with CISE and EUROSUR enables better coordination and cooperation among different national agencies involved in border management, leading to more effective border control measures.

Conclusion

NESTOR's next-generation holistic border surveillance system plays a crucial role in addressing the challenges faced by the European Community in managing its borders effectively. The system's long-range and wide area surveillance capabilities, combined with real-time fusion of border surveillance data and web and social media information, provide the relevant authorities with a more comprehensive and intelligent pre-frontier picture, enabling them to make more informed decisions about border control and response operations. Furthermore, the interoperability of NESTOR's system with CISE and EUROSUR is leading to better coordination and cooperation among different national agencies involved in border management, resulting in more effective border control measures. Overall, NESTOR's system will significantly enhance the European Community's border management and surveillance capabilities.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021851. 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

ODYSSEUS

ODYSSEUS - Unobtrusive Technologies for Secure and Seamless Border Crossing for Travel Facilitation

Monica Florea[1], Dana Oniga[1]

1. Software Imagination and Vision - SIMAVI

ODYSSEUS - Unobtrusive Technologies for Secure and Seamless Border Crossing for Travel Facilitation (https://odysseusproject.eu/) is an innovative EU project, funded under the Horizon Europe 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 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.

By offering very precise risk assessments, ODYSSEUS will allow civilians to pass the border without pausing, while also decreasing burden and improving productivity for Border Guard Authorities. ODYSSEUS will harness the power of digital technology to provide citizens with the tools they need to cross land and sea borders in a secure and seamless manner, while also providing border authorities with new tools for secure identity verification and unobtrusive vehicle/luggage/cargo checks, which will reduce long delays at border areas. Citizens would be able to traverse borders without any intervention by using their cell phones in conjunction with robust and ongoing identification verification. Authorities will be able to apply relevant controls remotely thanks to remote vehicle/luggage screening through X-Rays and UAVs.

The most significant technical outcomes of the project are the following technologies: Seamless Identity Verification at border crossing, Digital and Virtual Passport, AI-powered Continuous Behavioural Authentication, Non-Obtrusive and Safe X-Ray Technologies for Vehicle Scanning, UAV-Assisted Vehicle Scanning based on Thermal and High-Resolution Cameras, Faceless GDPR Compliant Travellers Counting, Multi-Modal Fusion and Decision Support System and X-AI for Privacy and Trust Enhancement.

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.

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 Sea 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. Face-recognition technology works with Mobile Passports, and UAVs fly over vehicles on board and those approaching port border controls to identify potentially unregistered travellers. In addition, vehicles entering and leaving the port are inspected using X-ray scanning to detect possible illegal/illegal goods and substances.

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, while border authorities can identify the travellers even the train is moving up to 80km/h.

The results that ODYSSEUS project will obtain will improve the border crossing experience for travellers and border authorities' staff, while maintaining security and monitoring of movements across land and water EU external borders, supporting the Schengen space, reducing illegal movements of people and goods across those borders and protecting fundamental rights of travellers.

Acknowledgements

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101073910. 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.

PARSEC

How detection technologies and new data sources can help re-design security controls for optimal parcel logistics - Vision of PARSEC project

Frank Janssens[1], Juha Hintsa[1], Toni Männistö[2]

1. CBRA Services
2. Cross-border Research Association

1. Challenges and PARSEC goals

Today, the use of detection technologies and risk assessment solutions is rather disconnected and fragmented: the approach of integrated detection architecture is missing in the postal and express domain. This lack of systemic approach complicates the detection of threat materials and illicit goods in postal and express courier flows. PARSEC project improves this situation by linking data-driven targeting processes more closely with the use of detection technologies. It also develops and tests next-generation non-intrusive detection technologies, which screening capabilities go beyond traditional X-rays, sniffer dogs, and material trace detectors in terms of detection accuracy, speed of screening, and range of threat materials identified.

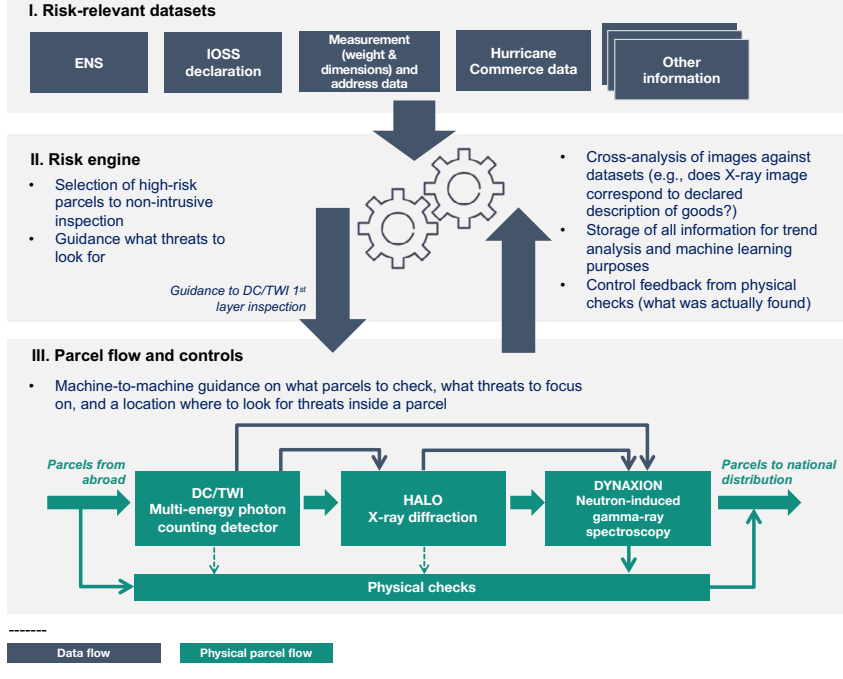
The PARSEC architecture or system-of-system will be modelled and optimized for both the logistics and detection goals, thereby combining the needs of postal and express operators versus customs and law enforcement agencies. Effective and integrated detection technologies, that are optimised for postal and express processes, will deliver higher capability for law enforcement practitioners and operators to detect threats and dangerous and illicit goods without disrupting the traffic of parcels and letters.

The project operates as an interdisciplinary faculty of security management, operations research, data science, applied radiography, applied particle physics, supply chain management, criminology, and innovation management. These disciplines

interrelate with the technologies of the four PARSEC innovation areas - data-analytics on combined data; multi-energy photon counting transmission and selected angle diffraction; full X-ray diffraction; and neutron-induced gamma-ray spectroscopy - and their combination into a PARSEC architecture.
PARSEC pools customs authorities and police as well as postal and express operators as end-user partners, and research and technology partners, in joint work. Methodologically such cross-disciplinary interaction works at best by doing real practical experiments. In PARSEC this is carried out through the three use-cases: Multi-threat risk assessment; Illicit drugs detection; and People safety to counter explosive and CBRN threats.

2. PARSEC architecture and integrated tools

By the end of the project, PARSEC aims to deliver a comprehensive blueprint, grounded on exhaustive engineering work and practical trials, on the total PARSEC architecture, consisting of following three key elements: risk-relevant datasets; risk engine with advance data analytics; and a process for controlling parcel flows with non-intrusive and physical inspection techniques.
The first element of the architecture, access to risk-relevant datasets, provides PARSEC partners the best available datasets on parcel flows, including declaration data, operational data from postal operators, and proprietary datasets from third parties like Hurricane Commerce.
The second element - the risk engine - integrates all this information and applies advanced data analytics to identify high-risk patterns in the data. With access to data on postal and express traffic, the risk engine allows customs and other stakeholders to identify high-risk parcels earlier and more accurately, and to determine which parcels should be selected to control and to what extent, where, when, and with which techniques the selected goods should be examined.
The third element of the architecture covers the physical flow of parcels and controls of high-risk parcels with non-intrusive detection technologies and physical checks. The PARSEC architecture will combine the data-driven risk assessment with the three stages of non-intrusive inspection technologies, multi-energy photon counting detector, X-ray diffraction screening, and neutron induced gamma-ray spectroscopy.
There are several interdependencies between risk-relevant datasets, the risk engine, and the parcel flow and control process. Risk-relevant datasets feed into the risk engine and provide raw data for preliminary selection of parcels for inspection. In other words, at this stage, the risk engine points out what parcels should be subjected to non-intrusive inspection and for what threats these inspections should look for. In the PARSEC architecture, the non-intrusive inspection technologies work in sequence, communicating to one another about parcels that require further inspection, what threats should be focused, and where inside a parcel, suspicious items may be located. There is a feedback loop of information between non-intrusive inspection and the risk engine: data from inspection stations will be used to cross-analyse, for example, whether X-ray images correspond to the goods that are stated in the customs declaration. This feedback is also used for trend analysis and machine learning purposes. The overview of the interlinked risk-relevant datasets, risk engine and non-intrusive inspection technologies is presented in the figure below.



Acknowledgements
This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101073963. This article reflects only the authors' views. The Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains. The authors would like to thank all PARSEC project partners for their contributions.

PROMENADE

PROMENADE - ImPROved Maritime awarENess by means of Artificial Intelligence (AI) and Big Data (BD) mEthods: Detection of abnormal behavior of vessels used for smuggling and drug trafficking in the Ionian Sea

Alkis Astyakopoulos[1], Christos Bolakis[1], Panagiotis Douris[1], Marios Moutzouris[2], Giovanni Laneve[3], Leonardo Millefiori[4], Antonio Bosisio[5] and Vasiliki Efstathiou[6]

1. Center for Security Studies, Ministry of Citizen Protection
2. Satways Ltd.
3. Leonardo Electronics
4. NATO Science and Technology Organisation
5. Transcrime, Università Cattolica del Sacro Cuore
6. Marine Traffic Ltd.

Maritime Domain Awareness is the combination of activities, events and threats in the maritime environment that could have impact on marine activities and affect the EU territory. During the past decades, advances in Information and Communication Technologies have provided a better means to monitor and analyse vessel activity. Today, private and public sources of data such the Automatic Identification System (AIS) or earth observation data can be combined with Vessel Traffic Services (VTS), Vessel Traffic Management Systems (VTMS) and Vessel Traffic Monitoring & Information Systems (VTMIS) data enabling the development of value-added information as a result of combining and fusing of such data.
European waters are navigated daily by some 12,000 vessels, which share their positions to avoid collisions, generating a huge number of positional messages every minute. It is important that this overabundance of information will not overwhelm the marine operator in charge of decision-making. The challenge is twofold: a) on one side the large-scale exploitation of heterogeneous data sources, enabling new Artificial Intelligence-based services for enhancing maritime situation awareness by means of automated processing in a way to minimise false alerts and b) on the other side the seamless integration and exchange of information among maritime surveillance authorities valorising the CISE network.

PROMENADE improves solutions for vessel tracking, behaviour analysis and automatic anomaly detection of vessels, using "state-of-the-art" Artificial Intelligence and Big Data techniques aiming at improving border and external security capabilities through an innovative, open and CISE-compliant service-based Toolkit. This reduces time to market, guaranteeing compliance with legal and ethical regulations and norms.

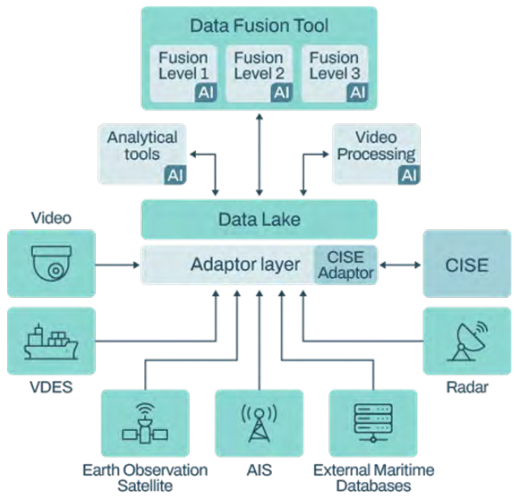
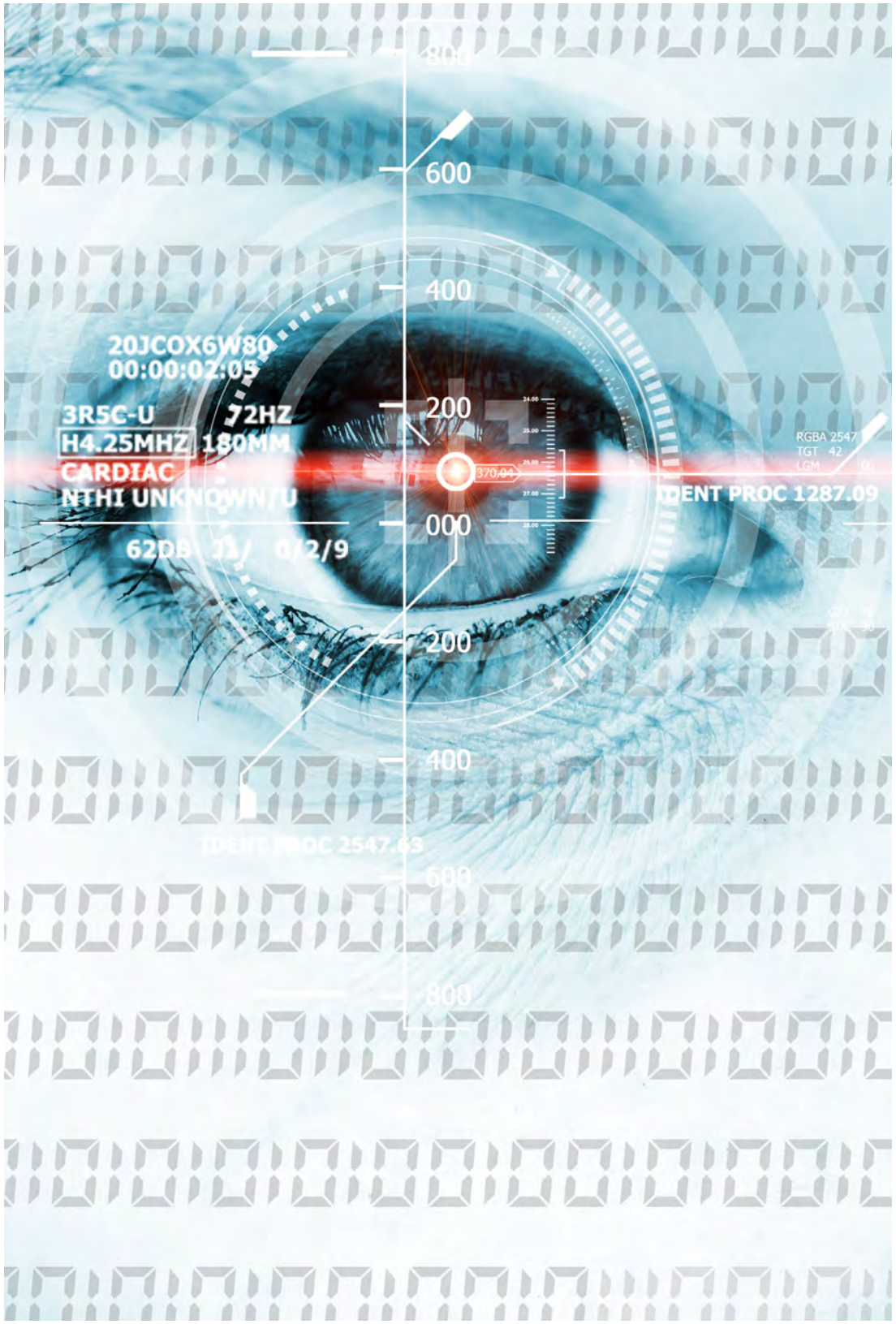


Figure 1. *PROMENADE High-level architecture*

At this end, PROMENADE developed a set of innovative AI/BD based services for improved Maritime Situation Awareness (MSA) grouped in five (5) main categories:
a) Classification services: they provide automated data processing and classification from various sources, including cameras, satellite imagery, and vessel tracking stations applied in the maritime domain, related to vessel detection, route classification, vessel activity classification and oil spill detections.
b) Pattern Detection services: they provide automatic pattern detection applied to multi-source data fusion, extraction of Patterns of Life, behaviour analysis and anomaly detection, AIS/Satellite analysis etc.
c) Risk Assessment services: they provide automated data processing and risk assessment of vessels' behavior and characteristics, through the use of innovative data sources and algorithms.
d) Future State Prediction services: they allow for learning the motion of ships in particular areas of interest from historical data with the goal of predicting their future trajectories and anticipating their future behavior.
e) Data Infrastructure which includes the data lake that provides the ingestion, storage, processing, and distribution of data in a Big Data environment and the data exchange with the external CISE Network in a plug and play manner.
It is worth mentioning that PROMENADE has used two different architectures to improve the obtained results and increase the performance of the Toolkit: (a) The Training architecture deployed as cloud computing infrastructure on top of Leonardo High Performance Computing (HPC) Davinci-1, providing virtualized services for developing the PROMENADE Data Lake, pipelines and training of AI services, and (b) The Operational architecture deployed at the end-users' premises for trials execution with the already trained services consuming real data and enabling communication with C2 Legacy Systems and CISE environment.
Throughout the PROMENADE project, one simulated trial and three physical trials of interest were conducted in Lithuania, Spain and Greece. The paper focuses on the results achieved during the Hellenic trial which aimed to test and validate the PROMENADE services by the Hellenic Coast Guard (HCG) in their operational activities in the Ionian Sea and specifically in Corfu straits between Corfu Island and Albanian coastline where activities of smuggling and drug trafficking are very common, as large amounts of narcotics are transferred to EU countries. For the Hellenic trial, the following services have been tested under operational conditions consuming data from various sources: TRITON Pattern Detection from Satways, Vessel Detection in Image Data and Vessel Tracking Pattern Detection from Leonardo, Advanced Ship Prediction provided from NATO-CMRE, Risk Investigator from UCSC and Multi-Sensor Data Fusion from MarineTraffic. On top of these software services and thanks to the PROMENADE project, a patrol vehicle of the Hellenic Coast Guard has been entirely renovated and equipped with innovative maritime sensors (radar, thermal camera, AIS, mobile C2 etc.) integrated in real time with the HCG Legacy System and PROMENADE Toolkit at strategic level enhancing maritime situation awareness.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021673. 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.



06

INCREASED CYBERSECURITY

HERMES

HERMES EDIDP project enhancing cybersecurity automation and information sharing in defence systems

Christos Skoufis[1], Marios Sophocleous[1], Frini Lazarou[1]

1. EBOS Technologies

The current state of cybersecurity faces various challenges that are impacting both civilian and military domains. One of the challenges is the underestimation of security requirements. Many organizations, including military entities, often do not fully understand the extent of security measures needed to protect their digital assets, leading to vulnerabilities that can be exploited by cyber threats. Another challenge is the underfunding of security implementations. Cybersecurity is often perceived as an additional cost rather than a crucial investment. As a result, organizations, including military agencies, may not allocate sufficient resources to implement robust security measures, leaving their systems exposed to cyber threats. Inherent vulnerabilities in components, such as software and hardware, pose another challenge. Despite efforts to develop secure systems, vulnerabilities can still be present due to coding errors, design flaws, or outdated technologies. These vulnerabilities can be exploited by cyber threats to gain unauthorized access or disrupt operations. The complexity of cyber threats is also a significant challenge. Cyber threats are constantly evolving, and attackers use sophisticated techniques to bypass traditional security solutions. This dynamic landscape requires constant monitoring, analysis, and adaptation of cybersecurity measures to effectively counteract emerging threats. Moreover, the increasing use of information and communication technology (ICT) technologies in defense capabilities, such as unmanned autonomous vehicles (UAVs), artificial intelligence (AI), machine learning (ML), and digital soldier concepts, introduce new complex threat vectors. These technologies, while offering significant advantages in military operations, also present new vulnerabilities that can be exploited by adversaries. Operational cybersecurity solutions are often added to existing systems as a temporary fix, resulting in information overload, poor data quality, lack of collaboration, and limited actionable intelligence. These challenges can hinder the effectiveness of cybersecurity measures and reduce the ability to detect and respond to cyber threats in a timely manner. Furthermore, the reliance on computers and electronic systems in the military introduces pressure points and unpredictability in future wars. Cyber threats can disrupt communication networks, compromise critical infrastructure, and compromise the confidentiality, integrity, and availability of sensitive information. This requires enhanced cyber readiness and resilience to effectively respond to and mitigate the impact of cyber-attacks. Overall, the current state of cybersecurity in the military domain, as well as in other sectors, is facing various challenges that require adequate recognition, investment, and proactive measures to ensure robust protection against evolving cyber threats. HERMES is a military-grade, enterprise system composed of different software components that are deployed in various parts of an organisation, including across security domains. It is used by various experts to gather, curate, and distribute cybersecurity information on the specific domain of autonomous military systems, and more specifically, unmanned ground vehicles (UGVs). The focus on UGVs is motivated by two factors, as presented below. Firstly, the strong and immediate operational requirement for cyber defence solutions that are as autonomous as the systems they are intended to protect. In this environment, data exchanges must be supported between distinct entities in demanding, complex, and high-security scenarios, a set of use cases that are well-aligned with the prior work on which HERMES is based. Secondly, the absence of adequate solutions in this specific area, implies that HERMES will be a blank sheet design developed with the latest knowledge and technologies. As such, HERMES exploited results will not have to expend effort to displace legacy systems whose effectiveness is inherently limited yet are propped up by powerful vested interests. Upon successful demonstration of its benefits in the specific area of the cyber defence of autonomous military systems, stakeholders will be better informed and will be more prone to view it as an opportunity for transforming legacy systems rather than a threat to existing business models. Ultimately, HERMES will help cybersecurity solution vendors as well as manufacturers and operators of autonomous military systems to work together more efficiently to better support autonomous cyber defence even in highly constrained and risky environments. HERMES aims to enable automation and autonomy in cybersecurity operations, improve controlled information sharing of high-quality cybersecurity

data, and facilitate burden-sharing collaboration and outsourcing of cybersecurity data management. Unlike traditional approaches that rely on interoperability standards, HERMES takes a disruptive paradigm shift by separating data representation, storage, and exchange from the uses made of exchanged data. It recognizes the complexity of exchanging cybersecurity data and offers a foundational system that can be used by all, providing common data representation, storage, and exchange capabilities. This allows applications to obtain data from a common system, saving efforts and resources, and enabling the development of better applications for specific needs. HERMES is referred to interchangeably as the "HERMES Data Exchange Platform" or "DXP," with the term "DXP" emphasizing its focus on data exchange across cybersecurity solutions, organizational boundaries, and security domains. HERMES outputs will be demonstrated through two use cases (UCs). The first UC is a general one showing the use of HERMES as a foundational data management service across multiple organizations. The second UC is more specific for the dissemination of cybersecurity data to autonomous military systems.

Acknowledgments

This project has received funding from the European Defence Industrial Development Programme (EDIDP) under grant agreement No "EDIDP-SME-2020-099-HERMES". This document reflects only the author's view. The European Commission is not responsible for any use that may be made of the information it contains.

IRIS

User-centric design and validation of a DLT/Blockchain-based auditing tool for incident response traceability and accountability

João Rodrigues[1], Gonçalo Cadete[1], Duarte M. Nascimento[1], Roland Kromes[2], Carmela Occhipinti[3], Lorena Volpini[3]

1. INOV – INESC Inovação
2. Cyber Security Group, Delft University of Technology
3. CyberEthics Lab

1. Introduction

Incident Response, in the context of disaster management, security and infrastructure protection, implies designing and executing automatic and semi-automatic response workflows. Enabling accountability of related actions is necessary to ensure that the relevant stakeholders operate in a risk-controlled environment.

Existing logging solutions for incident response workflows allow for some degree of assurance regarding traceability and accountability, by enabling post-incident analysis of the incident context and operators' actions. In the scope of the IRIS European Union's Horizon 2020 project, a Data Protection and Accountability (DPA) module was designed to support auditing functions for incident response, ensuring accountability and traceability based on a combination of distributed ledger technologies (DLT), blockchain, self-encryption, and secret key sharing technologies. The DPA enables secure, immutable, and resilient distributed logging for incident response workflows, optimized for cooperating networks of CERT/CSIRTs.

The DPA solution will be demonstrated and evaluated in two realistic pilots in two European smart cities, featuring scenarios of autonomous transportation vehicles and smart grid infrastructures. To assess the progress beyond the state-of-the-art, societal acceptance and design science research methodologies will be used to

elicit and validate the specific operational requirements of incident response stakeholders.

2. Data Protection and Accountability Solution (DPA)

The DPA enables the traceable, immutable and safe storage of audit data, with access control policies enforced by several nodes. It leverages the capabilities of the Hyperledger Fabric (HLF) permissioned blockchain to provide an auditing service that respects the societal, ethical, and legal implications of auditing procedures involving multiple organizations. The DPA consists of three sub-modules: the Hyperledger Fabric blockchain; the Crypto-tools; and an off-chain database.

Hyperledger Fabric is a private, permissioned blockchain whose architectural flexibility allows the DPA to be adapted to different enterprise architectures.

Crypto-tools is the sub-module of the DPA that enriches the HLF network with cryptographic self-encryption and secret key sharing capabilities.

Blockchain/DLT technologies such as HLF present performance challenges for constant storage of data, or storage of large amounts of data. Therefore, encrypted audit data is stored in a scalable off-chain database, mitigating the risk of the DPA becoming a performance bottleneck.

3. Conclusion

An effective accounting and traceability solution for incident response is crucial for enabling post-incident analysis of the incident's context and operators' actions. The DPA is an auditing solution designed for the aforementioned purpose.

A user-centric approach, that considers aspects of societal acceptance as well as the best practices of user-centric design, is essential to maximize the solution value and the exploitation potential in future operational deployments. From a social values standpoint, the DPA directly contributes at promoting accountability in automated and semi-automated incident response, by ensuring and furthering the core properties of information security (confidentiality, integrity, availability, authenticity, and non-repudiation). Although the desirability of promoting accountability in settings where high responsibilities are at stake may appear as prevailing and self-evident, from a user-centric perspective, value tensions may affect social acceptance (e.g., accountability-independence). Such an approach makes it possible to consider scenarios in which the accountability pressure may produce changes in users' behavior which are relevant to security - the non-repudiation property ensured by the DPA may inhibit actions which are riskier from the point of view of potential individual responsibility but that are more effective responses to threats. Furthermore, when adopting a socio-technical system perspective, the chance of exploring broader social implications may arise (e.g., changes in collective perceptions of avoidability, individual responsibility).

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 101021727. 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.

LAGO

A Generative Adversarial Network (GAN) Solution for Synthetically Generated Botnet Attacks Data Samples

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

1. School of Electrical and Computer Engineering, National Technical University of Athens
2. Department of Agricultural Economy and Development, Agricultural University of Athens

Abstract: The trend of digitization in almost every aspect of daily human life has raised serious concerns about security in the digital world. With new technologies, solutions, and tools emerging daily, new vulnerabilities also arise. Botnets are among the most widespread cyber-threats in the modern digital landscape, as they can breach and affect entire organizations or domains by infecting just a single device in a network. This study involves the design and implementation of a Generative Adversarial Network (the so-called ZDGAN) to synthetically generate botnet attack data samples, which are assessed for both quality and quantity using specific data quality indicators. The quality assessment results show that the produced data are very similar to the original ones. Therefore, the significance of GANs in data generation processes is almost undeniable. Furthermore, increasing the volume of annotated data can lead to the improvement and enhancement of AI-based cybersecurity solutions that heavily rely on data availability.

1. Introduction

The widespread adoption of digital services in people's daily lives has resulted in an increased demand for cybersecurity. With the proliferation of new software and hardware, detecting known vulnerabilities and zero-day exploits has become a daunting task for cybersecurity professionals. Botnets are one type of software vulnerability and attack that can have disastrous consequences [1]. These attacks allow attackers to remotely control infected machines. To combat these infections, cybersecurity experts are developing proactive systems that utilize machine and deep learning technologies. However, the lack of available training data often hinders the development of these systems. To address this issue, a new study proposes a methodology for generating botnet-type data in a tabular format. This methodology involves the use of Generative Adversarial Networks (GANs) [2] with varying parameterizations to determine the most efficient and reliable way to generate synthetic data with high accuracy while minimizing computational costs. The generated samples will be assessed using a wide range of Graphical Data Quality Indicators, such cumulative sums, absolute log mean and STD diagrams, correlation matrices, and heatmaps.

2. Proposed solution

Generative Adversarial Networks (GANs) [1] utilize an architecture that generates new data based on input data and random noise. GANs consist of two components: the generator and discriminator. The generator uses random noise to create realistic data, while the discriminator classifies input samples as either real or fake. Both components are optimized based on the discriminator's ability to accurately classify real and fake data.

This study aims to evaluate the effectiveness of different GAN architectures [2] in generating synthetic data that accurately represents malicious cyber-attacks, specifically botnet attacks. To accomplish this, the study compares the performance of different GAN architectures for both the generator and discriminator, using the CTU-13 dataset [3] from the Stratosphere IPS. This dataset includes captures of diverse malware samples and normal traffic, with 32 million packets. The training dataset has 216,352 records, with 140,849 marked as "0" for malware and 75,503 labeled as "1" for legitimate. The evaluation dataset has 88,258 records without any labels.

The study utilizes the ZDGAN model architecture [4], which is designed to generate 1D synthetic data from the input dataset. The model was implemented using Tensorflow 2.0 and Keras API. The proposed ZDGAN architecture utilizes the sequential API to stack the different layers of the deep neural network. The generator component includes an input layer that accepts scaled random noise, nine hidden layers activated by the 'ReLU' function, and an output layer activated by the 'linear' function, with the same dimension as the (preprocessed) dataset, i.e., nine feature columns. The discriminator model is also a sequential model with four dense layers.

The first three layers are activated by the 'ReLU' function, and the output layer is activated by the 'sigmoid' function to distinguish input samples as real or fake. A dropout rate of 20% was applied to the visible and two hidden layers of the discriminator model.

After detailing the generator and discriminator models, the proposed ZDGAN model is characterized as a sequential model that integrates these components in an adversarial manner. Figure 1 illustrates how the ZDGAN model uses (preprocessed) botnets data samples to generate synthetic, tabular data.

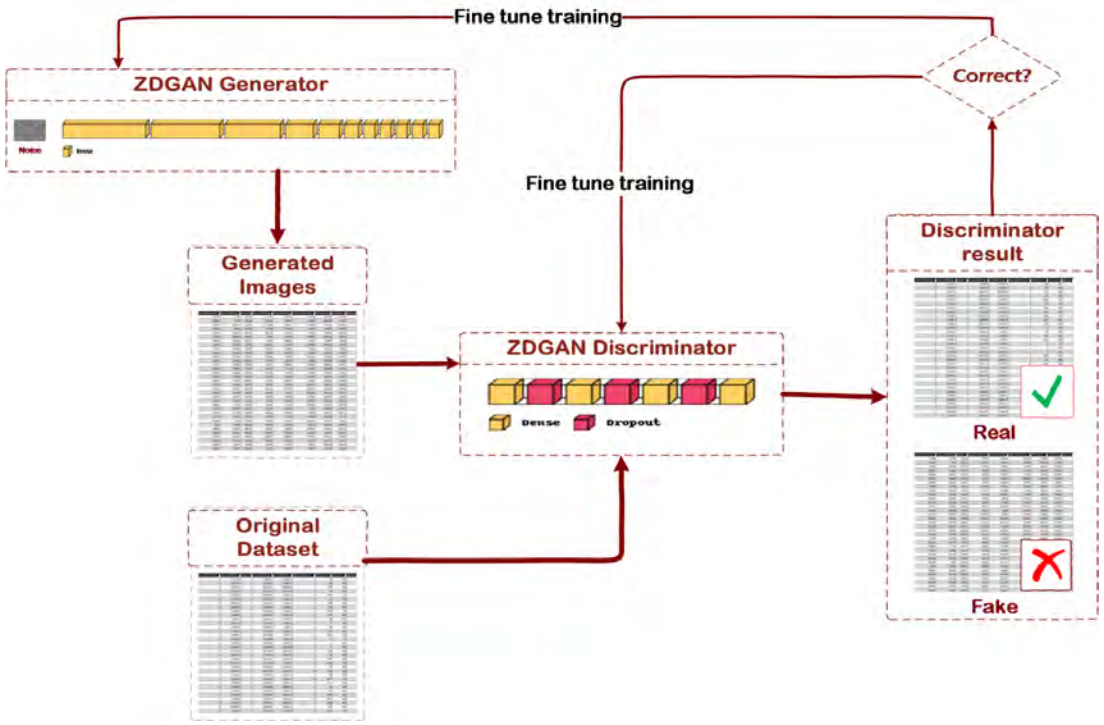


Figure 1. *ZDGAN Model Implementation*

3. Conclusions and Future Work

In conclusion, as digital tools continue to evolve and become more prevalent, the need for effective cybersecurity measures has become increasingly critical. The primary objective of this study is to outline a comprehensive methodology for generating synthetic data for botnet attacks using Generative Adversarial Networks (ZDGAN). The generation process utilizes an open-source dataset, the CTU-13 dataset [3], provided by Stratosphere IPS, which is a collection of network traffic captures that has been widely used in the field of cybersecurity research. This tabular format data is used as input for the suggested ZDGAN architecture [4]. The ZDGAN model generates over 200,000 new botnet data samples that closely resemble the original data. Subsequently, the generated botnet data samples are evaluated using a wide range of Graphical Data Quality Indicators, including cumulative sums, absolute log mean and STD diagrams, correlation matrices, and heatmaps, to assess the quality of the generated data. Overall, this proposed methodology provides a promising approach to improving botnet attack detection and prevention.

Acknowledgements

The work described in this paper is performed in the Horizon Europe project LAGO ("Lessen Data Access and Governance Obstacles"). This project has received funding from the European Union's Horizon Europe research and innovation program under grant agreement No 101073951.

References

1. Shinan, K.; Alsubhi, K.; Alzahrani, A.; Ashraf, M.U. Machine Learning-Based Botnet Detection in Software-Defined Network: A Systematic Review. Symmetry 2021, 13, doi:10.3390/sym13050866.
2. Randhawa, R.H.; Aslam, N.; Alauthman, M.; Rafiq, H.; Comeau, F. Security Hardening of Botnet Detectors Using Generative Adversarial Networks. IEEE Access 2021, 9, 78276–78292, doi:10.1109/ACCESS.2021.3083421.
3. García, S.; Grill, M.; Stiborek, J.; Zunino, A. An Empirical Comparison of Botnet Detection Methods. Computers & Security 2014, 45, 100–123, doi:https://doi.org/10.1016/j.cose.2014.05.011.
4. Peppes, N.; Alexakis, T.; Adamopoulou, E.; Demestichas, K. The effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers; MDPI Sensors, 2023; ISSN 1424-8220.

SANCUS

SANCUS

Konstantinos KALTAKIS

Eight Bells LTD

Extended Abstract

The project involves 15 Partners from 8 European countries, and aims to design and develop an analySis software scheme of uNiform statistiCal sampling, aUdit and defence proceSses (SANCUS – a Roman god of trust). The main idea draws on formalising the logic of expressing (for the first time) the notions of cyber security and digital privacy by means of final formulas and fuse them into optimisation strategies to acquire the truly optimum defence recommendation in dynamic manner, i.e., with respect to the runtime changes of the telecommunications network environment. In this respect, SANCUS will dimension new inclusive Key Performance Indicator metric, namely, the security-vs-privacy-vs-reliability efficiency trade-off, for measuring the system network cybersecurity and privacy performance explicitly, flexibly, automatically and agnostically. To realise the heterogeneity of the security and privacy levels across the system network and its supply chain, the proposed scheme sits on six efficient engines, namely, FiV, CiV, SiD, AcE, MiU and GiO, which combine unique modelling of the Internet of Things units, cuttingedge methods for automated firmware and software validation and verification, and innovative Artificial Intelligence driven game techniques for the automated optimisation of the control and trust of digital services. Extended evaluations of the project outcomes are also considered by means of developing contemporary network testbed prototype built on latest 5G and cloud-native system setting and running three pilot use cases for examining the scheme performance across Firmware, Virtualisation and Management software layers. The SANCUS scheme will be delivered as integrated software suite and it is expected to revolutionise the European research and development efforts, in and out, the cybersecurity regime. All outcomes are planned to be audited and disseminated extensively.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 952672. 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.

SECANT

Cyber Threat Intelligence in the healthcare domain: The SECANT approach

Arnolnt Spyros[1], Ilias Koritsas[1], Aggelos Papoutsis[1], Athanasios Dimitriadis[1], Dimitrios Kavallieros[1], Theodora Tsikrika[1], Stefanos Vrochidis[1], Ioannis Kompatsiaris[1]

1. Information Technologies Institute, Centre for Research and Technology Hellas

SECANT is an EU-H2020 project, which aims to deliver a holistic framework for cyber security risk assessment for strengthening the understanding of cyber security risks, at both human and technical level, and for enhancing the digital security, privacy, and personal data protection in complex ICT infrastructures. SECANT is developing an automated threat detection platform addressed to CERTs/CSIRTs that is capable of identifying threats and attacks, while promoting the situational security awareness as a priority within complex ICT infrastructures, such as the healthcare ecosystems by employing beyond the state-of-the-art technologies and methodologies.

Figure 1. *SECANT use cases*

SECANT comprises four major pillars which contribute towards the enhancement of the capabilities of organisations' stakeholders, providing: (i) collaborative threat intelligence collection, analysis and sharing; (ii) innovative risk analysis specifically designed for interconnected nodes of an industrial ecosystem; (iii) cutting-edge trust and accountability mechanisms for data protection and (iv) security awareness training for more informed security choices. The performance of the proposed solutions will be validated in four realistic pilot use case scenarios applied within the healthcare domain as depicted in Figure 1.

SECANT develops innovative risk analysis methodologies, which are capable of supporting public/private organizations and relevant stakeholders in the identification of risks, impacting the security and privacy of data, infrastructure and services throughout their ecosystem. Therefore, SECANT enables not only the protection of connected organisations in technological manner, but also empowering the users in better protecting themselves. Ultimately, SECANT will contribute decisively towards improving the readiness and resilience of the organisations as well as their users against the crippling modern cyber-threats, increasing the privacy, data protection, and accountability across the entire interconnected ICT ecosystem, while reducing the costs for security training in the European market.

The Threat Intelligence Module (TIM) of SECANT is responsible for the collection, extraction, and sharing of CTI from both several external (i.e., online), as well as internal sources. External sources include sources such as vulnerability databases, CERT feeds, databases with Proof of Concept (PoC) exploits, social media, forums, and relevant web pages from the Surface and the Dark Web. With regard to internal sources, TIM utilises different honeypot instances, while also enabling the automatic gathering of threat intelligence from logs and alerts as collected through other components of SECANT or directly from the security mechanisms of the end-user. TIM filters the collected data to avoid storing personal data, by leveraging rule-based techniques, and extracts CTI from the collected sources using rule-based and machine learning based techniques. Subsequently, the collected data is further analysed in order to identify possible correlations between the information collected both from external as well as internal sources (e.g., correlation between CPEs and CVEs), utilising both simple (e.g., MISP correlation) and advanced (e.g., ML-based) techniques. The collection process is achieved both (i) manually through a user-friendly GUI as well as (ii) automatically on daily basis from trusted sources, leveraging appropriate scripts and configurations.

In essence, the Threat Intelligence Module enables:

- Manual and automatic collection of information about threats and vulnerabilities from internal and external sources;
- Effortless incorporation of new sources of interest;
- Automatic extraction and enrichment of CTI;
- Automatic correlation; and
- Storing and sharing CTI.

Acknowledgements
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101019645.
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.

07

ENHANCING THE DEFENSE CAPABILITIES OF THE EU

ACTING

Advanced European platform and network of Cybersecurity training and exercises centres

Nikolai Stoianov[1], Emil Ivanov[1], Kristina Hristova[1]

1. Bulgarian Defence Institute

1. ACTING Project in a nutshell

The term "cyberspace" is becoming more and more popular, and it is used constantly but what is "cyberspace" and how it is related to military operations is not well-defined. The characteristics of cyberspace are not well understood by the wider public, and relationships with national security and military issues are not entirely explored and agreed in the EU. One of the reasons is that the "cyber" has become deeply central to almost everything the military does to protect national security interests. Another challenge is that a wide variety of actors operate in cyberspace. The EU has different responsibilities towards EU citizens, but exactly where that responsibility lies, and the extent of that responsibility is currently being debated.

ACTING Project delivers an organized and coordinated approach to strengthen proactive cyber defence operators training exercises of the European Union, through effective and efficient multi-domain collaboration and the development of advanced technologies to ensure exercises situational awareness, automatic performance evaluation and the capability to describe technology agnostic exercises via a description language. The Partners will execute on a 48-month work plan to develop, model and demonstrate a network of advanced interconnected (federated) domain oriented cyber ranges for training and exercises, incorporating sophisticated methods and techniques for simulation of users, analysis of the performance of the cyber operators, and scoring cyber security situational awareness, supported by leading-edge scenario development language.

The ACTING project integrates study, design, prototyping, and testing activities in the domain of cyber security covering:

- Simulated user method and technology – software agents that use the common and specific software applications simulating user behaviour.
- Automated performance analysis – tool that collects data about the cyber trainees, provides measurements and performance analysis (visual and numerical) as well as identifies directions for training improvement that needs to be done for a specific user.
- Scenario Development Language – tool capable to translate scenarios developed by consortium or external partners (EU CAIH, ECHO, Universities, Industry) to be integrated and understandable for federated cyber ranges as well as for human beings.
- Multi-domain simulations (Federated Cyber Ranges) – Extending and improving existing federation of cyber ranges (established under the H2020 ECHO project) 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.

In order to justify the capabilities of the proposed approach and resulting tools and platform, based on the Main High-level requirements and the 2018 CDP Priorities, 3 (three) representative defence-oriented use cases were developed. Use cases include (i) Combined cyber-attacks against joint Headquarters Land and Navy CIS systems; (ii) Space-Maritime (Transportation/Military) Sectors; (iii) Cascading effect for cyber-attack in civilian sector.

The use cases are based on credited scenarios and include a description of teamwork and the operational application of the ACTING tools and platform as a whole, with capabilities for organizing complex realistic large scale training and exercises covering several domains and sectors. In addition, ACTING will provide the coordination between other EU activities such as EU CAIH PESCO project, EDA's CD TEXP, and CySAP, EDIDP ECYSAP and H2020 ECHO projects. Last, but not least, ACTING will provide a framework, common standards and interfaces to interconnect existing cyber ranges, to develop technical and scoring elements of cyber defence scenarios taking as a source already developed use cases and scenarios from various external sources and projects (from Academia, Industry and EU Funded Projects) and build on top of this user performance scoring and common situational awareness system covering federated cyber ranges. For each of the use cases, ACTING

Project will develop a demonstration scenario and methodology proof of usefulness of the ACTING Platform. Each element will be validated by external domain experts and MODs representatives.

Acknowledgements

This project is co-funded from the European Union's European Defence Fund under grant agreement No. 101103208 — ACTING — EDF-2021-CYBER. 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. ACTING Grand agreement
2. https://acting-project.eu/

EU GUARDIAN

EU-GUARDIAN

European Framework and Proofs-of-Concept for the Intelligent Automation of Cyber Defence Incident Management

Nikolai Stoianov[1], Maya Bozhilova[1], Yantsislav Yanakiev[1], Valery Ivanov[1]

1. Bulgarian Defence Institute

1. EU-GUARDIAN Project in a nutshell

That we live in a digitalized era is a reality. Our banking, medical, communication systems, as well as the functioning of the military command are highly and progressively dependent on Information and Communications Technologies (ICT). Among the novelties, one of the most disrupting technologies is Artificial Intelligence (AI). Like the steam engine or electricity in the past, AI is transforming our world, our society and our industry. The growth in computing power, the availability of data and the emergence of new algorithms have turned AI into one of the most strategic technologies of the 21st century. In this sense, AI can help us to tackle many crucial challenges, including cyber defence and incident management. Through COM/2018/237, COM/2020/65 and COM/2021/206, the European Commission established EU's approach to AI centres on excellence and trust, aiming to boost research and industrial capacity while ensuring fundamental rights. Additionally, it is believed that AI will strengthen EU's potential to compete globally and will help build a resilient EU for the Digital Decade. AI will not only make our lives easier, but will also help solve some of the world's challenges.

Nowadays AI, machine learning (ML) and automation are revolutionizing the way IT teams approach complex and multi-faceted tasks. Cyber defence and incident response are no exception. For this reason, by providing new opportunities for addressing the inefficiencies that have traditionally plagued the cyberspace, AI promises to make it much easier to resolve more incidents, at greater speed, and with less effort. Indeed, just as the rise of technologies like cloud computing and containers over the past decade has allowed IT teams to deploy applications much more efficiently and with less manual effort. With the integration of AI, automation

has been taken a step further, providing cyber response teams with much faster root-cause analysis and algorithmic noise reduction. Incident management is one of the primary areas that benefits largely from this adoption since AI can help automate workflows for smarter and more efficient incident management, freeing up time for IT operations team members to focus on innovation improving user experience. But its adoption in real cyber response, and in particular in that related to Cyber Defence (CD) actions, is not exempt of challenges and barriers, not only technical but also social, economic or political. To name but a few of them: lack of AI related ICT skills and short-term learning strategies, inadequate levels and focus of investment in R&D on AI technologies, insufficient datasets and supportive data-driven enablers for ML and other AI tools, social perception of digitalization and AI as threats, or lack of EU and international agreements for related technological standardization and regulatory gaps. On these grounds the EU-GUARDIAN (European frameworks and proofs-of-concept for the intelliGent aUtomAtion of cybeR Defence Incident mAnagemeNt) project aims at creating an AI-based solution that operates and automates large parts of incident management and cyber defence processes. EU-GUARDIAN will focus primarily on the ability to detect, mitigate and respond to security challenges semi-automatically or automatically; support human operators, analysts and decision-makers at all levels; and contributing to enhance cyber situational awareness, military infrastructure resilience and protection against advanced cyber threats. This will be driven by improving prediction, optimising operations, better resource allocation, and personalising service delivery.

The basis of the project focuses on providing an innovative and more efficient solution that makes a radical contribution to incident management and cyber defence. The outcomes will support capabilities able to identify, plan and enforce the most suitable responses, increase their speed and accuracy, and strengthen overall security.

EU-GUARDIAN embraces this challenge by relying on the Divide and Conquer (Lat. Divide et Impera) paradigm, which addresses complex problems by gaining and maintaining AI-enabled power by breaking up larger concentrations of power into pieces that individually have less power than the one implementing the strategy, the latter referred in the context of the project to as metacognition layering. On these grounds, EU-GUARDIAN will implement the Divide and Conquer problem by defining a layered and hierarchical AI-based autonomous system. Each EU-GUARDIAN Autonomous Layer will be able to cover its own whole Observe-Orient-Decide-Act (OODA) loop under a combined cyber-physical and socio-cognitive situational awareness, which adapts its autonomy to the scientific method for solving cyber defence challenges; where Observe represents the acquisition of factual knowledge (evidences, performance indicators and symptoms), Orient shall guide the inference of new knowledge form the observed (diagnosis, suppress/surpass opportunities via readjustment, situational analysis, creation of playbooks, etc.), Decide will guide the response/adaptation choices (option analysis, valuation, prioritization, selection, and planning), and Act will enforce the adaptation and/or re-calibration actions.

The project differentiates six core automation stages (Data, Instrumentation, Situational Analysis, Response, Communication, and Metacognition), where the Metacognition Layer will represent the highest and most inclusive and holistic levels of AI consciousness and its relationships with significant other entities present thorough the operational context (technologies, effectors, plans, etc.). The base of the hierarchy will be constituted by the Data Layer, which shall adapt the procedures for adaptive management of the factual and inferred knowledge that shall feed the rest of the levels. EU-GUARDIAN has the potential to orchestrate the compliance with changing priorities as the mission and the operational context evolves per layer or as a whole system. Based on this, it will be possible to identify multiple KPIs (response time, quality of the decision, trust/strengthening of the algorithmic adopted, affordability in terms of resource expenditure, energy efficiency, etc.). Each Automation Layer operating as a whole can prioritize its performance based on them. The agnosticism and modularity within each layer will entail a core project cornerstone, since it is out of the EU-GUARDIAN scope to re-develop mature and satisfactorily tested/operative products and solutions, but explore new concepts on state-of-the-art gaps, while taking advantage of AI-based automation to Contextualize, Automatize, Suppress and Surpass its operation in order to enrich without modifying the original product, its effectiveness according to the circumstances.

Acknowledgements

This project is co-funded from the European Union's European Defence Fund under grant agreement No. EDF-2021-CYBER-R-CDAI-2. 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. EU-GUARDIAN Grand agreement
2. https://www.eu-guardian.eu/

CUIIS

Comprehensive Underwater Intervention Information System (CUIIS)

Nikolai Stoianov[1], Sergey Belkinov[1]

1. Bulgarian Defence Institute
1. CUIIS Project in a nutshell

The highly demanding underwater domain is characterized by its environmental factors like Sound Speed in Seawater, Temperature, Salinity, Pressure, Underwater Visibility, Underwater Sound Transmission, Sound Propagation Losses, which not only effect the functioning of any equipment, but has an adverse effect on the human beings and even the smallest mistakes could have extremely negative effect on their health condition.
In addition, in this harsh domain, a certain number of underwater threats (Submarines, Unmanned Systems, Mining and Combat Divers) operate concealed and are always hard to detect.
In this challenging environment, Consortium of 18 entities from 7 EU MS (Bulgaria, Denmark, Finland, France, Italy, Poland nd Romania), supported by 5 EU MS namely Bulgaria, Denmark, France, Italy, and Romania, is proposing an innovative 36 monts long project entiteled The Comprehensive Underwater Intervention Information and Support System (CUIIS), which is going to provide solutions to avoid/mitigate Decompression Sickness (DCS) risk, create and use a real-time underwater common operational picture through the fusion of various types of information and ensure interoperability, coordination and de-confliction of underwater intervention activities, including manned-unmanned teaming, involving employment of a big number of divers and UUVs simultaneously (swarm).
The CUIIS project integrates study, design, prototyping, and testing activities in the domain of:
• Decompression sickness mitigation strategies through the use of "smart" diving equipment
• Underwater Manned-Unmanned teaming
• Smart Hyperbaric Systems
• Diving Electronic Sensors and UUV Control
• Enhanced Underwater Communication and Information System (UWCIS)
• Tactical Command and Control
• Visual user interfaces for Underwater Innervation and Information System
The proposed modules of the CUIIS system are organized to respond to the call, to meet project goal, and to achieve sucesful results addressing project objectives.
The Comprehensive Underwater Intervention Information and Support System (CUIIS) is 36 interdisciplinary research and innovation efforts that will results in a comprehensive solution for enhanced defence diving to detect, identify, counter and protect against sub-surface threats, which consist of the following Subsystems:
The Smart Hyperbaric System (SHS) has a limited presence of medical hyperbaric chambers with a PLC controlled decompression system, where the environment is controlled and no continuous monitoring of the patient physiological parameters is used to correct the decompression curve or the composition of the air/oxygen mix.
For the Intelligent Diving Equipment (IDE), has been identified, that there is no diving computer or system on the market allowing monitoring in depth and in real-time diver health to improve the safety of decompression strategy. In addition, the current military rebreathers that are mainly in service are divided based on the depths and operations for which, they are used.
For the Unmanned Underwater Vehicle Subsystem (UUV) it was identified, that currently there is no possibility to integrate UUVs (ROVs and/or AUVs) into the diver security and operations and this Diver's/UUVs collaboration in mission management, communication, and underwater evolution is not developed.
At the moment in most missions there is no Enhanced Underwater Information Subsystem (EUIC) available between the divers and surface personnel. The Divers use mostly visual marks between each other and when safety ropes are used, they are used for messaging between the surface and the single diver.
In the area of Hand Held Devices (HDD), the picture of mission achievement, status, locations and critical information to the divers and commanders is not available at the moment.
For the Control Command Communication Subsystem (C3S) it was identified, that the C2 systems are focused on the management of military operations in all traditional areas, but the management of diver and UUV missions is not adequately presented, especially in the complex accumulation.

In order to address and solve abovementioned weaknes, the consortium is proposing solutions beyond the state of the art.
In order to justify the capabilities of the proposed system, based on the Main High-level requirements, 4 (four) representative defence oriented use cases were developed. Use cases include (i) Recovery of sensitive payload from sunken military aircraft in a contested underwater environment, the (ii) Defence of Offshore Platform as part of the EU Critical Maritime Infrastructure from underwater attacks (divers and UUV's), (iii) Active MCM Operation on focal points of the Sea lines of communication (SLOC) employing UUV's and Diver Teams and (iv) Employment of EOD Diver Teams and UUVs in support of Harbour Protection.
The use cases are based on creditive scenarious and include description of teamwork and the operational application of the CUIIS, with capabilities for providing real-time information about the status of the divers to the On Scene Commanders, in order to mitigate the risk of Decompression Sickness (DCS) by allowing the EOD Divers to stay in the search areas as long as possible, capabilities for constant localization and tracking of the EOD divers for tasks like precise search pattern following and decision making. In addition, the CUIIS will provide the coordination between the EOD divers and the UUVs. Last, but not least, the CUIIS will provide the on the Scene Commander (OSC) with the position of friendly divers and UUVs, ensuring that this information is distributed between the divers, participating in the operation, Naval vessels involved in the operation, thus contributing to the common operational picture. For each of the use-cases is included description of the demonstrations, which will be conducted during the project exection, as part of WP05 and WP06.
Based on the Mission analysis, number of factors (Purpose, Time and Space) and functions (Command and Control (C2), Situational awareness, Movement and Maneuver, Sustainability and Medical and Health Support) will be constantly evaluated and considered, since they are going to affect the general tasking of the system, size and weight of the equipment, electrical power consumption, precision of positioning, range of communication, integration, cyber security and etc.
The Project team envisages to demonstrate elements of the system during the bilateral annual exercise "Poseidon", which is MCM orientated, in which Bulgarian, Romanian and often SNMCMG-2 MCM vessels and EOD Divers participate, during which comments and remarks on the available CUIIS subsystems could be received, evaluated and implemented, if necessary.

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.

References
1. CUIIS Project Grand agreement
2. https://cuiis.eu/

FARADAI

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

1. FaRADAI extended abstract

AI technology has greatly impacted various aspects of modern society and economy. Recent technological advancements have significantly improved decision-making and support systems, as well as autonomous processes, by utilizing different types of data, such as text, visual content, and video footage. To provide accurate outcomes, AI models 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. Alternatively, Frugal AI approaches have emerged to address the data necessity issue, having as a main advantage the use of fewer data for training, as learning procedures entail very few samples, with the ultimate challenge being the development of a powerful model, capable to continuously learn with minimal human interactions and no intervention of experts.

Within the defence domain, data may be characterized as limited or incomplete, as well as sensitive in nature, requiring security clearance for proper labeling by dedicated personnel. Additionally, data may be specific to certain types of military sensors, such as infrared or multispectral sensors. When employing AI algorithms in military applications, it is essential that any recommendations and decisions made are compliant with safety and security regulations, considering the complex and continuously changing environment. Furthermore, an AI framework must be inter-pretable from the perspective of operators such as commanders.

The FaRADAI project aims to deliver new approaches, algorithms and tools as research products to address some of the most prominent issues relevant to AI applications and to increase their applicability and impact on defence systems:

• Frugal AI: To achieve high levels of accuracy when deploying an AI framework and exploit it as an asset in modern warfare, operation-specific data must be available. A major drawback in such a scenario involves limited availability of sufficient annotated datasets. Moreover, the majority of such data are 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). This reliability, however, is very likely to be affected by 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.

To tackle the aforementioned issues, FaRADAI proposes to:

o Develop frugal AI methods for reducing data total size to train and adapt 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 a model's performance with a very limited amount of data, while minimizing the expert's/operator's need to intervene in cases of reusing the models under different conditions. Leveraging from transfer learning techniques, the knowledge of existing models will be extended, while reinforcement learning will provide environmental adaptation, with an ultimate goal to produce an AI framework tailored to the requirements of defence scenarios.

o Develop robust and explainable models in order to increase the operator's confidence and trust. A variety of methods will be developed which include but are not limited to:

o Hybrid AI techniques by combining different basic and DL-based methods, discriminative, generative, and evolutionary learning.

o Methods for improving robustness against adversarial attacks. Enabling logic-based representations of reasonable model behaviors, defined and expected by the human operators.

o Explainability metrics and mechanisms for the analysis and explanation of the decisions made by the AI models.

o Provide a framework for enhanced planning and operational capabilities, through

the development of AI- based schemes, that will use fused multimodal data, obtained by heterogeneous sources, to extract additional knowledge. 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. Similarly, AI-powered decision-making tools will also be designed, developed and evaluated to-wards supporting mission planning and C2 in order to deliver an improved framework of situation awareness and intelligence.

The ambition of FaRADAI is to produce relevant research advances in the development of new technologies which will be successfully applied in the context of AI for defence applications, covering all stages of a military operation supply chain, from planning, to execution, C2, decision making, mission adaptation and resource allocation.

Acknowledgements

This project has received funding from the European Defence Fund programme un-der 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 au-thority can be held responsible for them.

FARADAI

Methodological Approach for Designing an Artificial Intelligence Repository for Defense Applications

Georgios Kampas[1], Marios Moutzouris[1], Leonidas Perlepes[1], Konstantinos Gyftodimos[1], Dimitrios Papageorgiou[1], Pantelis Michalis[1], Georgios Eftychidis[1], Antonis Kostaridis[1], Dimitrios Diagourtas[1]

1. Satways Ltd.

Artificial Intelligence has made great leaps of progress since the time of the Logic Theorist program (Simon, Newell, Shaw 1956) where a machine was created to think like a human. Since then there has been a continuous evolution of AI in terms of algorithms and the associated computing power required to make it possible. These days one of the core pillars of AI is data. Without data, AI cannot be trained and any inference is based on false information.. Defense organizations are using AI in different spaces such as detection, planning and field operations. The management of this data requires a structured storage area and thus designing and developing an AI repository for defense applications requires careful consideration of several factors. A well-designed AI repository needs to store and manage large volumes of data considering various parameters such as the type and volume of data to be stored, the purpose of the AI algorithm to be developed, the format in which the data is to be stored and to provide access to this data.

In most cases, the data must be annotated with accurate labels, and the labeling process should comply with ethical and legal standards. Appropriate data management practices shall be defined regarding cataloging, metadata, storage and documentation. Access to the data should be restricted and secured to prevent unauthorized use and potential security risks, while specific authentication mechanisms should be applied. Versioning is also important to capture the evolution of the data and finding changes to datasets and to manage incompleteness. Additionally, the

repository should follow community-endorsed interoperability best practices to facilitate data exchange and re-use within and across relevant disciplines, such as security applications, enabling the researchers to advance their scientific work with minimal barriers. Finally, documentation of the data provenance and quality assurance processes should be meticulously maintained to ensure transparency and reliability of the AI models developed from the data. All the aforementioned parameters should be taken into account to select the best possible design approach for any individual repository.

In the current paper, the methodological approach is defined and followed to design and develop an AI dataset repository in the context of the EU funded project FaRADAI, which is focused on frugal and robust AI for defense applications. To facilitate collaboration among the partners involved in the project, the FaRADAI Dataset Repository (FDR) will be developed and will serve as a central repository for the datasets and provide secure access to authorized users. The repository is designed according to predefined methodological steps that are further detailed below, considering all the different parameters affecting its design principles.

The methodology for designing and developing the FDR involves several key steps to achieve its main objectives. The initial methodological step focuses on the identification and collection of datasets from various existing sources to meet the user requirements and use case needs. The datasets may include non-cooperative and cooperative tracking data, ground, marine, and airborne electro-optical data, radio signals, and other relevant data sources.

Once the datasets are gathered, a thorough assessment is conducted to evaluate the quality and relevance of the data, as the second step. This assessment involves examining factors such as data accuracy, completeness, consistency, and data source reliability. It ensures that the selected datasets meet the desired criteria and are suitable for the intended AI algorithms and applications.

Data preparation is a crucial, third, step that follows the assessment of data and involves cleaning, preprocessing, and transforming the datasets to make them suitable for AI algorithms. This process includes but is not limited to tasks such as data cleaning, normalization, and data formatting to ensure consistency and compatibility across different datasets.

Before storing the data, it is of utmost importance to clearly articulate the purpose of the AI algorithms that will be applied to the datasets. This involves identifying the specific objectives, tasks, or analyses that the AI algorithms will perform on the data. Defining the purpose of the algorithms contributes to the design of the repository and organization of the data in a way that aligns with the intended use cases.

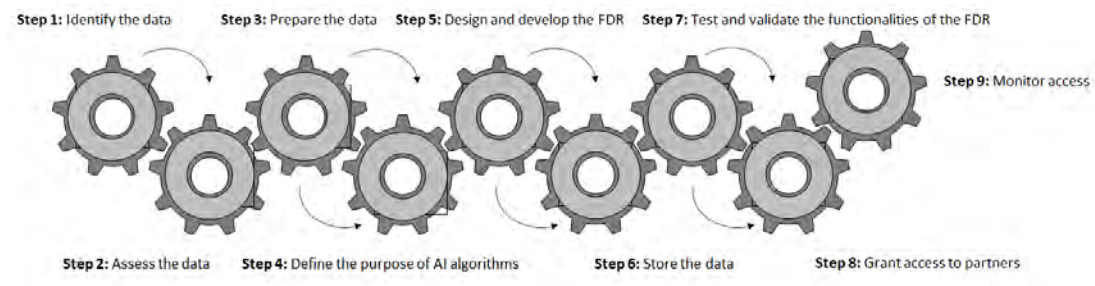
This fifth step involves the actual design and development of the FDR. The repository is designed according to the principles defined in the previous steps as well as to the chosen repository characteristics, including scalability, security, metadata management, versioning, data transfer, and collaboration features. The development process includes implementing the necessary software components, user interfaces, and backend infrastructure to support the repository functionalities.

The collected and prepared datasets are stored in the developed FaRADAI Dataset Repository. The repository should provide secure and scalable storage infrastructure capable of accommodating the volume and diversity of the collected datasets. Proper data organization, indexing, and storage practices are implemented to ensure efficient data retrieval and management.

The seventh step follows the development phase, where thorough testing and validation of the FDR functionalities are performed. This involves conducting several tests to ensure that the repository functions as intended, including dataset uploading and downloading, metadata management, searchability, access control, versioning, and collaboration features.

Once the FDR is tested and validated, access is granted to the intended users. User roles and access rights are defined, allowing authorized partners to securely access and collaborate on the datasets stored in the repository. Proper access controls and authentication mechanisms are implemented to ensure data security and privacy.

Once access is granted to the users, the final step includes the monitoring and tracking of users' activities within the FDR. This foresees implementing logging and auditing mechanisms to record user interactions, including dataset access, downloads and modifications. By monitoring access, any unauthorized activities can be detected, ensuring in parallel the security and integrity of the data.



By following the aforementioned methodological steps, as also illustrated in the diagram above, the design and development of the FDR can be carried out effectively and ensure the availability and accessibility of the relevant datasets for analysis and collaboration.

Acknowledgements
This project has received funding from the European Union's European Defense Fund research programme under grant agreement No. 101103386. Views and opinions expressed are however those of the authors 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.

References
1. The Age of With – The AI advantage in defense and security", Deloitte Analytics, 2021.

FIBERSENSE
Using fiber optical cables for maritime situational awareness

Dimitris Diagourtas[1], Pantelis Michalis[1], Aggelos Vassileiou[1], Charalampos Papadakos[1], Marios Moutzouris[1], Souzanna Sofou[1], Spyros Antonopoulos[1], Kyriakos Alevizos[1], Bernd Drapp[2], Matthias Mildner[2], Thomas Hamm[2], Paulo Chaves[3], Armando Fernandes[3], Max Goerler[4], Ivor Nissen[4], Vassilis Karastathis[5], George Drakatos[5], Dimitris Venizelos[5], Aggelos Mouzakiotis[5], Konstantinos Papagiannakis[6], Victor Lobo[7]

1. SATWAYS Ltd
2. AP Sensing GMBH
3. INOV Instituto De Engenharia De Sistemas E Computadores Inovacao
4. Wehrtechnische Dienstelle Für Schiffe Marinewaffen Maritime Tecnologie Und Forschng
5. National Observatory of Athens
6. Greek Navy

1. Project Summary
1.1 Introduction
The project "Using fiber optical cables for maritime situational awareness" (FIBERSENSE) will focus 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 will be 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 FIBERSENSE Concept

FIBERSENSE 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. FIBERSENSE will try 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 FIBERSENSE solution's design will be based on three core elements:
1) The FOC will serve as the sensing element.
2) The DAS Interrogator will measure the reflected wave.
3) The Data Collection Platform will collect, process and analyze further the DAS output to produce meaningful results.
Several feasibility studies will be performed in 3 test sites (Portugal, Germany and Greece) that will include:
- 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

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

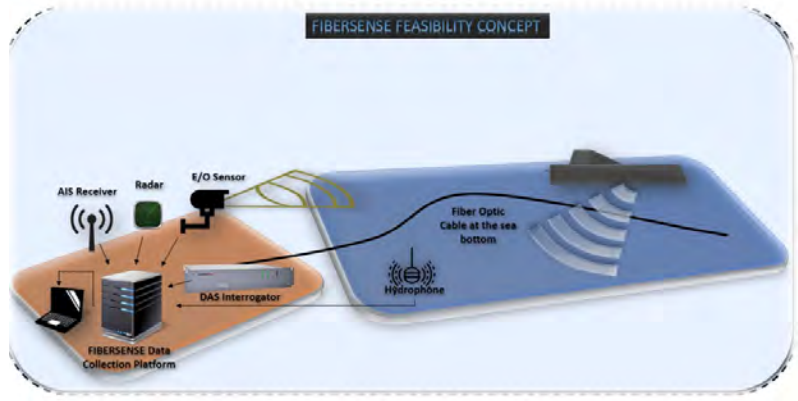


Figure 1. *FIBERSENSE Feasibility Studies Schema*

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.

KOIOS

The role of end-users in the development of AI applications for Defence

Francisco Andrés-Pérez[1,2]

1. CT Engineering Group
2. University of Salamanca

Abstract

End-users' involvement in the co-design of Artificial Intelligence applications has been identified as a critical premise to assure requirements addressing human-centered approaches such as trust, human control or explainability. The current presentation aims to show methods, techniques and tools that allow users of software systems, who are acting as non-professional developers, to create, co-design, modify or adapt AI applications. The work has been developed with the support of the European Defence Fund (EDF) under the framework of an international collaborative research project on the development of Artificial Intelligence methods for Defence Use cases (KOIOS[7]). This project aims to develop a community of practice to set representative defence use cases to test AI methods in terms of trustworthy, frugality and rapid adaptation. A human centered approach, integrating ethical concerns and end-user's needs, has been proposed to adapt the application of AI in a socio-technical defence domain.

1. Introduction

The term 'end-user development' has acquired a broader meaning covering approaches, frameworks and socio-technical environments that allow end-users to shape digital artefacts that encompass both software and hardware technology (Barricelli et. 20019). The complexity of Artificial Intelligence algorithms and their impact on decision-making has broadened the interest and need for a revision of human-centered approaches. The rapid evolution of AI technology has generated much excitement about its potential to improve process or make better decisions. However, it has raised as well serious concerns about the lack of human control or unintended consequences. The participation of end-users in Defence Applications is even more critical than in other domains due to the impact of their decisions and the uncertain environment in which they move. The failure of large complex systems to meet their deadlines, costs, and stakeholder expectations are not, by and large, failures of technology. Rather, these projects fail because they do not recognize the social and organizational complexity of the environment in which the systems are deployed. The consequences of this are unstable requirements, poor systems design and user interfaces that are inefficient and ineffective. On top of that, the nature of defense applications which are sensitive to AI technology aids is to rely on rapidly unpredictable situations by humans. Related user-cases are given, for instance, in situational awareness scenarios due to natural hazards, with high impact in civil and military actuations. Social experiments based on human factors and socio-cognitive methodologies to extract needs, requirements and main constraints (data, transferability...) based on participatory methods will be applied in the project.

The human-centric perspective holds that true intelligence can ultimately be found only in human beings and (potentially) in other living creatures. AI can help humans to reach their full potential but will not be able to develop certain essential qualities found in humans, such as moral reasoning or empathy. Traditionally and still in military operations, humans and automated systems have fulfilled complementary but separated functions within military decision making (Hosack, Hall, Paradice, & Courtney, 2012). Some concepts have been developed to represent the integration of AI in human decision-making: "meaningful human control" is used to encompass legal, moral, ethical dimensions while "effective human control" addresses performance or risk reduction. (Butcher, 2018)

7 KOIOS: Knowledge Extraction, Machine Learning and other AI approaches for secure, robust, frugal, resilient and explainable solutions in Defence Applications. See https://edrin.org/fileadmin/media/Factsheet_EDF21_KOIOS.pdf

Acknowledgements

This project has received funding from the European Defence Fund under grant agreement No. 101103770. This article reflects only the authors' views and the DG-DEFIS and the European Commission are not responsible for any use that may be made of the information it contains.

References

a) Barricelli, B. R., F. Cassano, D. Fogli, and A. Piccinno. 2019. "End-User Development, End-User Programming and End-User Software Engineering: A Systematic Mapping Study." Journal of Systems and Software 149: 101–137.

b) Butcher, M. B. (2018). An Exploration of Maintaining Human Control in AI Enabled Systems and the Challenges of Achieving It. NATO.

c) Hosack, Bryan; Hall, Dianne; Paradice, David; and Courtney, James F. (2012) "A Look Toward the Future: Decision Support Systems Research is Alive and Well," Journal of the Association for Information Systems, 13(5).

08

ARTIFICIAL INTELLIGENCE

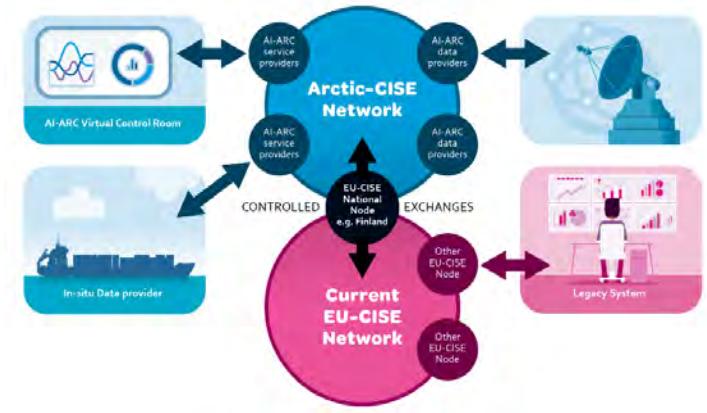
AI-ARC

Maritime AI services in the Arctic

Isto Mattila[1]

1. LAUREA UAS

The AI-ARC project will develop a shared collaboration workspace based on innovative and efficient AI services, a VCR (Virtual Control Room) that will significantly enhance border and external security, as well as support cooperation managing external borders in the Artic and High North Seas. The platform will be tested and developed together with practitioners and other end users in order to properly address their needs. The new technological solutions to be developed rely on existing systems, in compliance with EUROSUR. Further, the platform is integrated with the CISE environment to ensure a seamless cross-sector and cross-border interoperability. This ensures a quick uptake of the platform by the practitioners, and the platform does not require costly investments or increased workload. Finally, AI-ARC pays specific attention to societal resilience and aims to improve citizens´ perception of safety too.



Modern maritime navigational, surveillance, and communications systems, combined with today's network technologies and data storage and sharing capabilities have created enormous amounts of available data collected from vessels and sensors operating worldwide. Currently, however, all of this available data does not necessarily reflect reality or help maritime operations. In fact, it presents two core problems.

The first problem is that threats and other significant maritime events of interest are often lost and hidden in regular traffic patterns due to these vast amounts of data. This presents a need to develop an intelligent data processing functionality that highlights unusual and inconsistent behavior (also called an anomaly) within this large data set. Creating these functionalities and increasing automation at higher fusion levels would support maritime operators with limited resources by giving them access to information such as early warnings about approaching threats.

The second problem is that due to these advancements in network technology and storage capacities an enormous amount of data is now available to the various maritime user communities. All of this data has the potential to create a comprehensive knowledge base from which to operate. However, without intelligent filtering of data, there is a risk of information overload, the operational picture getting over complicated and decision-making efforts delayed or impaired. The consequences are potentially dramatic in terms of accidents, pollution, border infringements, and criminal activities and are possibly further aggravated in areas so remote as the High North Atlantic, Arctic, and the upper High Norths which are not monitored as closely as other European waters. This presents an urgent need to create an intelligent filtering and retrieval mechanism to navigate this dataset.

The main objective of the AI-ARC proposal is to create an innovative, robust, efficient, and user-friendly artificial intelligence (AI) based platform that meets and exceeds the above-mentioned needs and provides powerful levels of situational awareness for decision-making and safety for all maritime actors without increasing workload. To achieve this objective the AI-ARC Consortium will use AIS, Copernicus, VDES, and other data sources to inform and build a Virtual Control Room (VCR). The VCR will incorporate machine learning technology, plus real and virtual reality (VR) components that combined will create a mixed-reality (MR) visualization layer and high-performance user interface, usable from different perspectives such as Coast Guards' or civilian users' and will be tested in both the Arctic and the Baltic Sea.

Within the VCR, the AI and machine-learning solutions will be applied to border/

coast guard surveillance data and operate by learning from validated statistical and near-real-time data, including user feedback. To take advantage of this technology, end users require advanced levels of visualization and interactions with a user interface. The VCR will visually help end users assess the risk of a given situation by flagging detected features with confidence and providing threat or risk levels according to a predefined and customized gradient model based on user preferences. This means that users can create a mixed reality environment for their own purposes that reflects their needs.

Additionally, the VCR will permit users to specify their preferences in terms of risk management, threat levels, abnormal behavior, and interoperability, and will incorporate reliable system responses with scalable time and place factors in different information layers. These functions enable the user to easily visualize and manipulate different data layers in near-real time using predictive analysis technology. These capabilities create a revolutionary 'smart' situational awareness picture and provide anomaly and non-compliance detection capabilities to the coast guard and border authorities as well as providing an adaptive risk allocation capability to every seafarer. As such, the VCR provides exponential maritime risk assessment capabilities to the larger maritime community and intends to become a valuable new tool for not only seafarers but also ship owners and the insurance industry.

- Collaboration across any network connection
- Homogeneous view from different devices
- Web based software allows to share situation with a simple link
- Hardware table as a team workspace
- 3D Data and remote collaboration using virtual reality

Of note, the AI-ARC project follows the requested CISE guidelines for information sharing. The concept behind Maritime CISE is to ensure that maritime surveillance-related information collected by one maritime sector/actor, which is considered necessary and useful for the activities of other maritime actors can be rapidly exchanged (following the CISE principle "responsibility to share"). Therefore, CISE is creating the optimal conditions for information collected by any maritime actor for a specific purpose, to be easily and securely accessed by another maritime actor performing a different mission.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021271. 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.

ALIGNER

ALIGNER
Developing a research and policy roadmap for AI in support of law enforcement

Daniel Lückerath[1*], Donatella Casaburo[2], Peter Svenmarck[3]

1. Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS
2. KU Leuven Centre for IT and IP Law (CiTiP) – imec
3. Totalförsvarets forskningsinstitut

Introduction

The world is changing at an unprecedented rate, and Artificial Intelligence (AI) is at the forefront of this change. While providing numerous benefits, many have raised concerns over the impact AI has or will have on matters such as security. The EU-funded ALIGNER[8] project aims to unite European actors who have concerns about AI, law enforcement, and policing to jointly identify and discuss how to enhance Europe's security whereby AI strengthens law enforcement agencies (LEAs) while providing benefits to the public.

To achieve this goal, ALIGNER has established expert groups from policing and law enforcement, civil society, policymaking, research, and industry, who work together in regular workshops to identify opportunities and risks arising from law enforcement use of emerging AI technologies, which capability enhancement needs are associated with the increased use of AI (both by LEAs and criminals), and which ethical, legal, and technical/operational impacts the deployment of AI technologies by LEAs might have. The results from the expert discussions are published in ALIGNER's AI roadmap, which provides recommendation to actors from policy, practice, and research how to tackle current and future challenges associated with AI technologies.

Assessing AI technologies for LEA use

To provide a basis for the work of ALIGNER's expert groups, a sound methodological approach is necessary for identification of promising (emerging) AI technologies for LEAs and their potential implications. ALIGNER therefore pursues a collaborative technology watch process, followed by a series of assessment workshops (technology impact assessment, risk assessment, ethical and legal assessment) as shown in Figure 1.

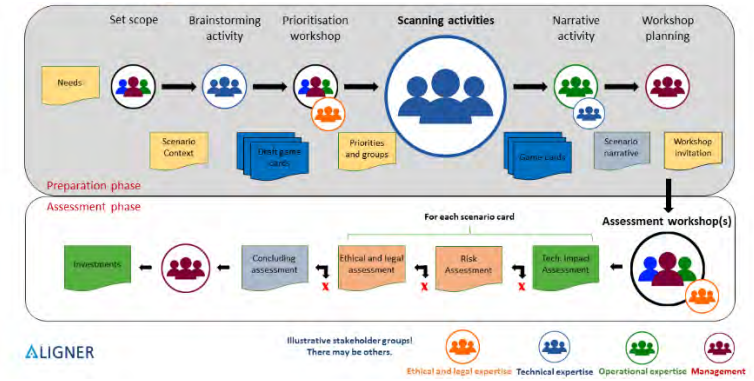


Figure 1. *The ALIGNER technology watch and assessment process. In grey: Technology watch process; in white: the assessment process*

The technology impact assessment (Westman et al., 2022) – based on a method developed in (Peters et al, 2019) – consists of two dimensions for assessment: added value and feasibility. The added value dimension measures in what way an AI technology will improve LEA capability, while the feasibility dimension measures how likely it is that the technology will work as advertised/intended. The dimensions are assessed using six and eight criteria, respectively, that are designed to be easy to understand and applicable to a wide range of AI technologies. Each criterion is assessed on a simple four-point scale. The scale has an even number of steps to make participants take a clear stance, either for or against the technology. Participants rate the criteria individually or in small groups and then discuss them jointly to identify misunderstandings and different perspectives.

AI technologies that have achieved a significant score in the technology impact assessment go through a risk assessment (still under development). If the technological/organizational risk from the deployment of an AI technology is reasonable, the ethical and legal impacts of deploying the AI technology are assessed using ALIGNER's Fundamental Rights Impact Assessment (FRIA, see Casaburo & Marsh, 2023). The FRIA should be conducted by teams of LEAs, legal and technical experts. The FRIA consists of two connected and complementary templates: 1) The Fundamental Rights Impact Assessment template, which helps LEAs identify and assess the

8 https://aligner-h2020.eu/

impact of their AI systems on those fundamental rights most likely to be infringed; and 2) The AI System Governance template, which helps LEAs identify the relevant ethical standards for trustworthy AI and mitigate the impact on fundamental rights. Only AI technologies that achieve suitable scores in all assessments should be considered for deployment at LEAs.
Within ALIGNER, exemplary assessments are conducted of promising AI technologies for different scenarios (e.g., identifying and countering misinformation, countering fraud and malwares). These results are then published within the ALIGNER AI roadmap, together with further insights into the capabilities enhancement needs of LEAs when employing AI and how research and policy might address these needs (see Lückerath & Wischott, 2023).

Acknowledgements
This paper has been prepared in the framework of the European project ALIGNER – Artificial Intelligence Roadmap for Policing and Law Enforcement. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101020574.
The sole responsibility for the content of this publication lies with the authors. It does not necessarily represent the opinion of the European Union. Neither the REA nor the European Commission are responsible for any use that may be made of the information contained therein.

References
1. Casaburo, D., & Marsh, I. (2023). ALIGNER D4.2 – Methods and guidelines for ethical & law assessment. H2020 ALIGNER, GA no. 101020574.
2. Lückerath, D., & Wischott, V. (2023). ALIGNER D5.5 – First Update of the Research Roadmap for AI in Support of Law Enforcement and Policing. H2020 ALIGNER, GA no. 101020574.
3. Peters, C. E., Grönwall, C., Bronkhorst, A., & Adlakha-Hutcheon, G. (2019). From foresight to impact for technologies at low technology readiness level. In Proceedings of the 13th NATO Operations Research and Analysis (OR&A) Conference: Challenges for NATO OR&A in a Changing Global Security Environment. NATO STO-MP-SAS-OCS-ORA-2019. NATO Science and Technology Organization.
4. Westman, T., Svenmarck, P., & Chandramouli, K. (2022). ALIGNER D3.1 – Impact Assessment of AI Technologies for EU LEAs. H2020 ALIGNER, GA no. 101020574.

ALLIES
AI-based framework for supporting micro and small Host Service Providers on the report and removal of online terrorist content

Serena Bianchi[1]

1. SYNYO GmbH

1. The Online Terrorist Content (TCO) growing trend
Despite the fact that the number of terrorist attacks has remained relatively consistent in recent years (119 in 2020 and 2019, and 129 in 2018), the internet has emerged as a significant factor in the dissemination of extremist propaganda. One of the most dangerous misuses of the internet for public security has been the spread of terrorist content on social media and websites. Directive 2017/541 defines terrorist content as any material that constitutes a "public provocation to commit a terrorist offence at its source." The publication of such content not only encourages terrorist acts but also facilitates the recruitment of supporters, training, and financing of terrorist acts, all of which are not restricted by location. To address this issue, Directive 2017/541 urges Member States to collaborate with third countries to remove such content or block it from the EU territory. The Internet industry has also been called upon to prevent such misuse of their services, albeit on a voluntary basis. However, the European Union has taken a step further by adopting a new regulation, the TCO Regulation (Regulation (EU) 2021/7845), which requires online hosting providers to remove any illegal terrorist content within one hour after receiving an official removal order.

1.1 About ALLIES Project
The ALLIES project AI-based framework for supporting micro and small Host Service Providers on the report and removal of online terrorist content) aims to assist micro and small Hosting Service Providers (HSPs) in adhering to the TCO Regu-

lation by providing them with learning, training, experience sharing mechanisms, and AI-based technical tools. The project's outcomes will not only contribute to the enforcement of the TCO Regulation but also align with the objectives of several other EU legislative acts and strategic documents. Specifically, the project aims to enhance the early detection of potential terrorist attacks, mitigate the use of the internet for extremist propaganda, and promote the usage of AI technologies for identifying online terrorist content. These objectives align with the EU Security Union Strategy's goal of protecting Europeans from terrorism and organized crime. The ALLIES project mainly targets micro and small HSPs in partner countries and beyond. This group was selected because they face significant obstacles in meeting the TCO Regulation's new requirements and guidelines due to their limited financial and operational capacity. The project seeks to raise awareness among these HSPs about the TCO Regulation and its requirements, assist them in implementing the regulation through the development of an AI tool, increase their knowledge capacity through training, and provide a safe online environment for experience sharing and reporting.

Acknowledgements

This project has received funding from the European Security Funds under the topic ISFP-2021-AG-TCO from the EU Home Affairs - Grant Agreement No 101080090. 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 European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

1. Europol (2021), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, accessed 02.01.2022.
2. European Parliament, Briefing EU Legislation in Progress, Addressing the dissemination of terrorist content online.
3. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHAOJ L 88, 31.3.2017.
4. Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.
5. Directive (EU) 2017/541 of 15 March 2017 on combating terrorism, OJ L 88/6, 31.3.2017.
6. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156/43, 19.6.2018.
7. European Council (11.12.2020), European Council meeting (10 and 11 December 2020) – Conclusions, EUCO 22/20 CO EUR 17 CONCL 8.

APPRAISE

APPRAISE - Facilitating Public & Private Security Operators to Mitigate Terrorism Scenarios against soft Targets

Anastasios Dimou[1], Petros Daras[1], Jorge García[2], Peter Leškovský[2], Olivier Balet[3]

1. Information Technologies Institute, Centre for Research and Technology Hellas (CERTH)
2. Vicomtech Foundation, Basque Research and Technology Alliance (BRTA)
3. Defense & Security Business Line, CS GROUP

In recent times, soft targets such as shopping malls, airports, transport systems, squares, streets, and sports events have become frequent targets for terrorist and criminal attacks. These attacks have been designed to cause maximum casualties, chaos, and social impact, and they have underscored the vulnerabilities of public venues. Several high-profile attacks, including the Manchester Arena attack in 2017, the Barcelona attack in 2017, and the Sri Lanka bombings in 2019, have further emphasized the need for effective mitigation strategies. Such attacks are often coordinated and simultaneous, and they follow deployment tactics that make it challenging to prevent or respond to them effectively. Additionally, victims of these attacks are often not immediately aware, which makes it challenging to mitigate the damage. To address the challenges posed by soft target attacks, it is necessary to bring together all stakeholders, including law enforcement agencies, security professionals, and the public, to achieve real-time holistic situational awareness, predictive competencies, and zero-latency intervention. By leveraging technology and data analytics, we can identify potential threats before they occur and respond promptly to minimize casualties and prevent further harm. There is a growing trend in Europe where public spaces are being owned or operated by private companies, resulting in the increased presence of private security staff. In fact, there are approximately 2 million private guards in Europe, with 1.5 million in the European Union. These private guards are often deployed in locations where Law Enforcement Agencies (LEAs) or other public authorities are not present on a permanent basis. LEAs and private security entities have complementary resources for surveillance, management, and communication. Therefore, effective cooperation between them can significantly benefit the protection of European citizens, creating a public-private security continuum that extends the monitoring and response capabilities to all urban spaces, whether they are publicly or privately operated and whether they are open or gated. However, the full potential of this collaboration has not been realized yet due to several barriers. To overcome them, better operational collaboration among LEAs, private security personnel, and citizens is essential. Information exchange needs to provide immediate situational awareness and coordination actions to both LEAs and private guards to enable fast and effective intervention during security incidents. Efficient communication channels are necessary to collect live field data, such as wearable sensors for private personnel, and crowdsensing, and to exchange information with the public during an attack. Additionally, collaborative training activities are crucial to create synergies between the public and private sector. Ultimately, active cooperation should create a mutually beneficial environment where both sectors can contribute to the safety of the public and create an environment where people can work, play, and live without fear of security threats.

The use of technology in collecting data from various sources such as CCTV systems, smart city sensors, and online activities has become increasingly common. However, the vast amount of data that is collected poses significant challenges for public and private security practitioners. They must be able to extract useful intelligence from this data in order to prevent security threats and protect the public. Public and private security practitioners may have different capabilities to analyze and interpret this data. Therefore, the full potential of the data may not be realized due to a lack of collaboration and resource sharing. Moreover, the integration of public and private sector resources raises ethical and legal issues, particularly in terms of data usage, accuracy, and impartiality. To address these concerns, new intelligent and privacy-respecting real-time Big Data applications are needed. These applications must be designed to facilitate efficient and proactive law enforcement, with a focus on behavior analysis, anomaly detection, and predictive analytics. The development of these applications requires the establishment of protocols to ensure the accuracy and impartiality of the data analysis, as well as to protect individual privacy.

APPRAISE will develop and validate a state-of-the-art framework for soft target protection with a particular focus on active, audited and well-defined information and intelligence exchange among private and public sector security practitioners

to enable an effective collaboration, at the information and the operational level. APPRAISE aims to revolutionize the protection of soft targets by integrating: (i) a scalable, flexible, and efficient Data Intelligence platform for threat detection, (ii) actionable Threat Intelligence to proactively detect vulnerabilities and analyse imminent and on-going crimes or terrorist attacks, (iii) soft target risk assessment based on both web content, social media analysis and on-site sensor data, (iv) instant situational awareness to plan and execute mitigation actions and (iv) collaboration capabilities to collaboratively mitigate incidents from the earliest stage of their detection. The APPRAISE framework will be co-designed with Social, Ethical, Legal, and Privacy (SELP) experts, introducing novel approaches (edge data processing, federated intelligence, responsible AI, risk-based information sharing) to ensure compliance with EU data privacy framework, confidentiality requirements and societal acceptance.

APPRAISE proposes a novel globally integrated, inclusive, collaborative approach to soft target security by analyzing and sharing data from existing smart systems, services, and detection systems. Social, ethical, legal, and privacy observatories will ensure that the tools developed meet EU legislation and are accepted by citizens. To detect physical and cyber threats, APPRAISE offers solutions such as video analysis for CCTV networks, wide area surveillance from drones, and audio sensors for detecting terrorist acts. Crowd-sensing capabilities will also be used to collect information from nearby people. The data processing tools are deployable at the edge or a local fog level to ensure GDPR compliance. APPRAISE will offer advanced tools to security practitioners, including online content analysis, soft target risk assessment, actionable threat intelligence extraction, smart data visualization, and AI-based decision support. The online content analysis module will acquire data from both surface web and darknet sources, perform a multi-modal analysis, and extract indicators of imminent attacks on specific soft targets. A social network analysis will be performed to identify networks and individuals orchestrating attacks or propaganda campaigns. The output of the threat detection and online content analysis modules, along with smart city data, will be visualized on a digital twin-based hypervision system for real-time situational awareness. AI-based Big-Data tools will be used for geospatial analysis, threat intelligence, and predictive analytics, providing advanced Decision Support Services. APPRAISE focuses on improving collaboration between private security practitioners and LEAs through enhanced information exchange and operational cooperation. The project will establish a secure framework for sharing data in a standardized structure, with access management and auditing procedures in place to ensure proper use of information. Private operators will have access to a simplified version of the hypervision system. Most importantly, APPRAISE will offer an AR framework for private security personnel to improve cooperative mission management capabilities. AR glasses worn by the private practitioners will allow for easy access to event information and guidelines while enabling in-situ data collection for better operational picture by LEAs. APPRAISE will consider diverse soft targets in terms of accessibility, existing security measures, infrastructure, people concentration, criticality level, and societal impact to create a holistic approach. The project will be demonstrated in four pilot sites: a tennis tournament in Italy, a cycling tour in France and Spain, an international fair in Poland, and a mall in Slovenia. APPRAISE will analyze various kinds of attacks, including terrorist and criminal attacks such as coordinated attacks, gun attacks, knife attacks, and cyber-attacks. The project will also consider emerging threats like rogue drones and fast-moving vehicles targeting public spaces.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021981. 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.

CAESAR

Integrating Safety and Cybersecurity through Stochastic Model Checking – CAESAR

D. Faure[1]

1. Thales R&T France

In a context of growing cybersecurity threats, the number and impact of cyberattacks has increased drastically in recent years and all information systems (IS) are exposed to these threats. The security industry follow this carefully. As a result the CAESAR consortium believes that self-learning detection, using machine learning, will be necessary to anticipate the impact and minimize the damage of cyberattacks on IS by triggering alerts as quickly as possible.

The CAESAR project will be deployed first in the banking sector. CAESAR will develop a non-intrusive cyber detection solution using self-learning algorithms based on an intrusion detection system composed of probes and a central server to receive and analyze information from probes already marketed by the French company Gatewatcher but not adapted to the field of banking application.

Smart security – this activity looks at combining the strengths of Binsec and Netzob. The aim is to obtain a more "intelligent" fuzzing with knowledge of the structure of the target program and with suitable controlled traffic generation. A current challenge is that the activity is very resource intensive. In this project there is 80% code coverage of the modules considered.

We are also looking at the increased detection of unlisted malware. One model is based on fuzzy hashes. There is a strong time constraint: it must be able to quickly analyze dozens of files per second. Each binary file is associated with a fuzzy hash which, unlike a classic hash, has the advantage of giving different hashes but close for two similar files. This makes it possible to calculate the similarity between two original files (via the Levenshtein distance or variant) and is suitable for machine learning. The second detection model, currently under development, will handle the case of undetermined files. It will be based on the similarity of assembly code, more precise but slower.

Finally, we establish the tests in the context of Cyber Banking Security. A traffic generator replicates client endpoints and servers across different types of protocols and applications. It is able to reproduce a real-world network infrastructure by generating legitimate and malicious traffic at the same time. This allows us to run functional tests, performance tests and security tests. Test benches are developed by Thales that include banking scenarios of the BNP Paribas. BNP Parisbas will consider this cybersecurity solution on their network to study the implications with respect to their Computer Security Incident Response Team.

HOLOZCAN

An AI-supported platform to detect airborne bio-threat

János Pálhalmi[1], Anna Mező[1]

1. DataSenseLabs Ltd

1. Introduction

An extensive amount of effort has been put into the development of different sensor solutions to detect, identify and monitor airborne biological agents. The variety of methods behind the several sensor solutions cannot go unnoticed, but no standard and interoperable EU-wide approach is available to set the threshold for monitoring critical infrastructure.

Regarding the currently available solutions for pathogen detection there is a trade-off between time and accuracy. While the gold standards for genus and strain level identification are still the different genomic methods, the classical optical methods like different forms of quantitative phase imaging microscopy powered by deep-learning or machine-learning offer the possibility of rapid and automated detection of suspicious pathogens either in water or air-based samples.

One of the reasons why there is no existing standard and interoperable bioagent monitoring solution is the lack of platforms capable of comparative data monitoring and archiving for traceable inter-method comparison.

Since disease control authorities are highly vigilant regarding the environmental presence of the most dangerous and unfortunately well-known member of the Bacillus cereus group, and it is very easy to access all the necessary components to create a virulent Bacillus anthracis strain, our AI supported platform is currently being finetuned for the detection of bacillus form objects sampled from the air.

2. Methods

The bacillus form object detection AI-supported platform is currently based on four different components sequentially following each other: 1. air sample collection; 2. sample preparation; 3. optical microscopic measurement; 4. AI-supported pathogen detection. In the current phase of the study the optical microscopic measurements were carried out by the DHM (digital holographic microscope) sensor manufactured by the EU Horizon supported HoloZcan project and by a reference DIC (differential interference contrast) microscope.

The performance of the DataSenseLabs AI-platform solution was finetuned and tested on two different sample types: laboratory made mixture of different bacterial strains including Bacillus subtilis (ATCC 6533); and environmental field samples collected by the Coriolis Compact air-sampling device manufactured by Bertin Technologies. The details regarding the standardization of the sample preparation, data collection, database building and the measurement technology will be discussed during the conference presentation.

3. Results and Conclusions

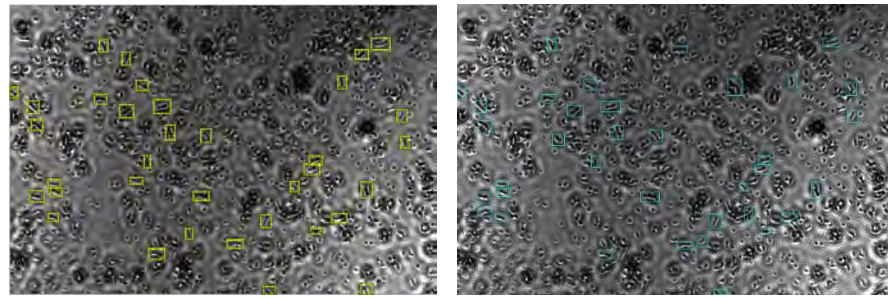


Figure shows the DHM images of Gram-stained laboratory mixture of strains (Bacillus subtilis ATCC6533, Enterococcus faecalis ATCC29212, Candida albicans ATCC14053) containing the reference annotation (ground Truth) marked by yellow rectangles on the left, and the Deep-Learning network model-based predictions marked by green rectangles on the right. Image dimensions: 1013 x 682 pixels (X, Y). Overall size of the image: 202.6 Qm x 136.4 Qm (X, Y).

overall accuracy	precision	recall	F score
95.74%	0.8060	0.8333	0.8194

The table shows the results of the Deep-Learning network model-based predictions regarding the presence of suspicious bacillus form objects in the laboratory made mixed sample.

The platform, as a first step, supports the quantitative phase imaging sensor-based data input for analysis and algorithm training. The algorithm system can detect and monitor the anomalies in the concentration of bacillus form objects sampled from the air with higher than 90% accuracy depending on the study design and sample type.
The integration of the platform into CBRN related further research, decision-making and pre-standardization will be presented during the conference.

Acknowledgements
The project was supported by Horizon 2020 programme: HoloZcan (GA: 101021723). (https://datasenselabs.net/ https://datasenselabs.net/horizon2020/)

popAI

The popAI methodology for systemising knowledge on the ethical use of AI in Civil Security

Dimitris Kyriazanos[1], Xenia Ziouvelou[1], Pinelopi Troullinou[2], Katrina Petersen[2], Gemma Galdón-Clavell[3], Paola Fratantoni[4]

1. National Centre for Scientific Research "Demokritos"
2. Trilateral Research Ltd
3. Eticas Research & Consulting
4. Zanasi & Partners

1. Extended Abstract

1.1 Introduction

pop AI is a 24 month EU H2020 Coordination and Support Action, bringing together security practitioners, AI scientists, ethics and privacy researchers, civil society organisations as well as social Sciences and humanities experts aiming to boost trust in AI by increasing awareness and current social engagement, consolidating distinct spheres of knowledge, and delivering a unified European view and recommendations, creating an ecosystem and the structural basis for a sustainable and inclusive European AI hub for Law Enforcement Authorities (LEAs).

1.2 The popAI methodology

popAI employs a variety of methods to reach its ultimate objective: to engage citizens and LEAs in order to improve their perception of security, produce ethically sound guidelines for future use, and foster a human-centred and socially driven AI for security. This is achieved through a three-phases process: ethical taxonomies, stakeholder attitudes, and co-created guidelines (Figure 1).

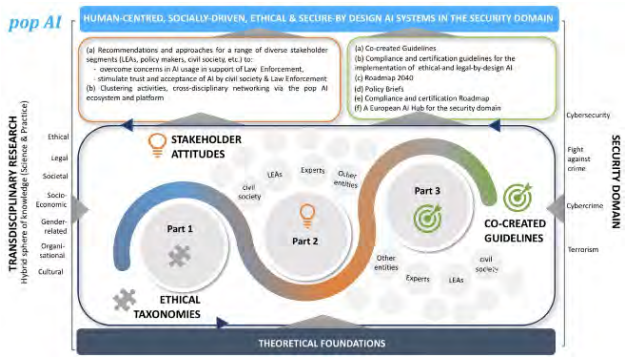


Figure 1. *The high level view of popAI methology*

First, popAI has built a novel taxonomy of ethical principles in the LEA/AI space, grounded in high-level ethical and human rights concerns and controversies around the use of AI in a range of policing contexts. This is done through desk research and engaging partner expertise in the field. Of specific interest is how AI is actually used, from organisational issues faced by LEAs to the representational challenges of the data that trains it; upcoming legal frameworks; the controversies around gender and diversity bias and discrimination that shape public discourse; and the ethical tensions that underpin the AI potential in the security field. Exploring issues such as the impact of organisational settings in technology adoption and success, practical ethics, human-machine interaction from a health and safety perspective, the consequences of AI on innovation and the job market, wage inequality, or procurement potentials, and a focus on technical specifications ground this phase in a novel approach to understanding the challenges of introducing AI tools in police forces in a variety of contexts, and incorporating technical challenges in a broader context of human and socio-technical dynamics. This phase is designed as a feedback loop of knowledge production, clustering, networking and stakeholder engagement.

Second, popAI conducts a multi-disciplinary analysis of experts and citizen awareness and acceptance through different forms of stakeholder and citizen engagement. This analysis is structured around capturing different levels of stakeholder engagement in these discourses: passive, active, and proactive in order to ensure popAI captures more than just the loudest voices but also the grassroots and emergent concerns. Such a structure to reach stakeholders supports different cultures of engagement and of voicing attitudes, creating a range of pathways that give voice to those culturally less inclined to speak in diverse settings (often the case of women and minorities) while supporting popAI in understanding which kinds of networks engage women, minorities, and more vulnerable populations in the innovation ecosystems in sustained ways. In order to complement the assessment around the controversies from the literature and broaden the stakeholder and innovation ecosystem maps, we explored the public discourse in the media. Media discourse is a powerful indicator of societal awareness and acceptance of new technologies. It both reflects public perception and shapes it. A scan and analysis of this discourse around the taxonomy and controversies identified is therefore key to grasping the general public's views and level of awareness of AI in the security domain. This also allows popAI to build an understanding of citizens who have opinions but are more passively involved (e.g. those that comment on social media but might not otherwise participate in shaping innovation trajectories or policy). In order to engage with LEAs and experts, a series of 5 one-day Policy Labs were organised. These labs gathered relevant stakeholders, multipliers, and intermediaries, including, but not limited to, LEAs, ethics experts, technology designers, policy makers, and included representatives from civil organisations that represent vulnerable and marginalised communities' groups. The end results are expert validated public policy recommendations and scenarios relevant both at regional and EU levels.

Third, based on the results of the desk-based research and the stakeholder engagement, popAI integrates the insights gained from citizens and LEAs and makes proposals and guidelines to enhance the ethical and legal frameworks for AI in policing. popAI produces a roadmap for AI implementation, and develops ethical sensitivity tools for LEAs, citizens, and policy makers. These outputs of the project include a practical set of insights that will allow the security sector to be better equipped to plan, develop, and implement a human-centred and socially driven AI successfully and responsibly.

Acknowledgements

popAI project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101022001. 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. popAI website: https://www.pop-ai.eu/

STARLIGHT

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

Jorge García[1], Roxana Pelin[2], Peter Van De Crommert[3], Nizar Touleimat[4]

1. Vicomtech Foundation, Basque Research and Technology Alliance (BRTA)
2. Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC)
3. Dutch Institute for Safe & Secure Spaces (DISSS), representing Netherlands Police
4. LIST Institute, CEA Paris-Saclay Nano-INNOV

Law enforcement agencies (LEAs) now have access to vast amounts of data, which was previously unprecedented. This has been viewed as a great opportunity for LEAs to solve and predict crime, but despite the big-data revolution, they have been unable to make the most of this data. Artificial intelligence (AI) is seen as a solution to many of society's challenges, such as increasing productivity and efficiency, identifying patterns, and making decisions quickly and accurately. In order to maximise the benefits of AI, LEAs need to adopt a human-centric and inclusive approach alongside a coherent data strategy to ensure the safety and security of society.

Data is vital for AI solutions. Technologies have made it easier to create, store, and distribute data. Social media, smartphones, and IoT devices track our daily interactions and store them on cloud services worldwide. LEAs also have interlinked datasets through investigations, historical cases, and databases. These datasets contain structured and unstructured text, multimedia, and relationship information in multiple languages, which poses a challenge but also an opportunity for AI adoption. LEAs, security practitioners, and others face these challenges daily. New operational capabilities powered by AI are needed to fight against (cyber)crime and terrorism. Solutions must be developed to address threats such as the spread of terrorist and sexually explicit content, trafficking, cybercrime, and attacks on public spaces.

Law enforcement agencies must be supported in their efforts to gather, analyse, and act upon evidence quickly and effectively. Proactive operations that enhance situational awareness, detect patterns, and enable investigative hypotheses are also crucial. As LEAs incorporate AI into their investigations, developed tools must enhance operational capacity, promote interoperability, and foster cooperation. Tools should be easy to integrate, solve problems instead of creating them, and facilitate information sharing and best practices. A sustainable community should work to build better AI solutions for LEAs across Europe through collaboration.

AI used in law enforcement poses legal and ethical challenges. It must be transparent and able to explain decision-making processes. Though AI is used in many LEA environments, its accuracy and specificity are often insufficient. The best-in-class AI solutions are dominated by organisations, who have unrestricted access to vast quantities of high-quality, structured, and labelled data. Europe must address the lack of legislation and coordination to advance research and operational AI, including regulatory, legislative, ethical, and security concerns. Access to data would drive investments and funding opportunities for EU research. Criminals can use AI technology to amplify existing threats and introduce new ones, requiring LEAs to be equipped to respond to these changes. Advanced technology requires enhanced cybersecurity operations, including the use of AI to detect cyber threats. However, all AI systems must be protected to maintain trust, as attackers can exploit their complexity through adversarial AI. A nucleus of AI stakeholders, researchers, and industry professionals should be brought together to promote a strategic and synchronised vision of AI for LEAs at the EU level. Collaboration with civil society and policymakers is also necessary to understand the societal implications of AI adoption and build trust. A dedicated hub is needed to unify AI knowledge, resources, and data for LEAs across Europe and promote long-term AI innovation, adoption, and uptake.

STARLIGHT aims to play a leading role in the effective use of AI for security in Europe. To better prevent, detect, and control crime, LEAs should use AI technologies to protect citizens and public spaces and increase resilience. STARLIGHT supports innovation and awareness of AI's potential benefits and risks for security and aims to create a European approach to AI for LEAs. By providing LEAs with automated, operational, and cyber-resilient capabilities, STARLIGHT will help tackle traditional and emergent criminal activities, terrorism, cybercrime, and cyberattacks in Europe. To achieve this, STARLIGHT aims to establish a strong EU AI-based security industry with interoperable AI solutions that uphold ethical and societal values to tackle

high-priority threats for all LEAs across Europe. Cooperation between researchers and security practitioners will ensure fast and effective uptake and adoption while aligning with legal and ethical provisions, legislative frameworks, and fundamental rights. STARLIGHT will ensure that European LEAs are at the forefront of AI innovation, autonomy, and resilience, prioritising the safety and security of Europe for all through the following strategic goals:
(i) To improve LEAs' knowledge of how AI can enhance their operational and cybersecurity capabilities at both EU and national levels.
(ii) To enhance LEAs' AI capabilities for predicting, preventing, detecting, and investigating criminality, terrorism, and border security while protecting digital infrastructures from cyber threats.
(iii) To develop a cybersecurity strategy and measures to protect AI LEA solutions proactively against cyberthreats (including trustworthy AI).
(iv) To enhance LEA's ability to investigate, combat, and prevent the criminal use of AI, including terrorism.
To transfer knowledge between LEAs, researchers, industry, SMEs, and policymakers, a strong ecosystem is required. It should facilitate an open exchange of the challenges LEAs face with their workflows, duties, and system requirements, as well as ideas on how AI can address these challenges. STARLIGHT's central goal is to build a strong, long-lasting ecosystem that facilitates trustworthy exchange and productive AI technology transfer. The ecosystem will be built around an AI framework that enables the participation of all stakeholders. Informed by end users' requirements and AI Community of Expertise stakeholders, the STARLIGHT framework will include cutting-edge AI/ML and data-driven technologies for (i) creating excellent multilingual and multimodal training and testing data in compliance with legal and ethical regulations at both national and European levels; (ii) using advanced and resilient AI/ML methods and tools to understand both physical (sensors and data-gathering devices for robotics and IoT systems) and cyber worlds (online sources from Surface/Deep Web, Darknets) and generate knowledge and intelligence in an explainable, transparent, and accountable way, by handling large volumes of multimodal data through fusion, correlation, and analysis. (iii) enabling LEAs to analyse, predict, detect, and mitigate cyberthreats and attacks, including adversarial AI.
STARLIGHT will deliver the following main results:
(i) A sustainable European AI Community, bringing together relevant stakeholders from the security and AI domains to foster adoption of AI technologies in the daily operational activities of LEAs.
(ii) A strategy for creating high-quality European training and testing datasets. This will include novel technological solutions for creating and annotating datasets, privacy-preserving measures for training and testing AI tools, and legal and ethical considerations for easier data creation and sharing.
(iii) A STARLIGHT Framework for trustworthy, accountable, responsible, and transparent LEA AI solutions. This will cover all technological needs of LEAs in AI, including machine learning, machine reasoning, natural language processing, robotics, and IoT. It will allow analysis of a wide range of (hybrid) threats and incidents.
(iv) AI-based cybersecurity and protection of LEA AI solutions, to improve cybersecurity operations and protect AI solutions against adversarial attacks.
(v) Detailed pilot scenarios tailored to real operational needs. The project is extendable to address additional areas and challenges posed by the LEAs and Europol.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021797. 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.

CO-ORGANIZING PROJECTS

Acting
ALIGNER
ATLANTIS
COURAGEOUS
CUIIS
ERATOSTHENES
EU-CIP
EXERTER
INHERIT
IRIS
MEDEA
METICOS
NESTOR
ODYSSEUS
PARSEC
popAI
PRAETORIAN
promenade
Search & Rescue
SECANT
SILVANUS
STARLIGHT
STRATEGY
VALKYRIES
EU-HYBNET
FaRADAI
FIBERSENSE
Firelogue
fireEURisk
FLEXICROSS
HERMES
HOLOSCAN
Melchior
MULTIRATE
SANCUS

WITH THE PARTICIPATION AND SUPPORT OF

European Commission
EUROPEAN UNION SATELLITE CENTRE
EARTO

CORE ORGANIZING GROUP

satways
iti Information Technologies Institute

Organizing Committee:

Ilias Gkotsis, Satways Ltd.
George Eftychidis, Satways Ltd.
Dimitris Diagourtas, Satways Ltd.
Stefanos Vrochidis, Information Technologies Institute - Centre for Research and Technology Hellas
Dimitris Kavallieros, Information Technologies Institute - Centre for Research and Technology Hellas
Nikolai Stoianov, Bulgarian Defence Institute

MAY 29-31, RHODES, GREECE

SECURITY AND DEFENSE 2023
CONFERENCE

The "Research and Innovation Symposium for European SECURITY and Defense"

www.rise-sd2023.eu