D6.7

Increasing Visibility of EU Security R&I projects

EU-funded Civil Security Projects Catalogue

by

6.3 task leader Research Council of Lithuania

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

Contents

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

Executive Summary

Safety and security play a very important role in today's society. Both safety and security are very important aspects of every country and ensuring the high level of security is a priority of many European countries. As in recent years modern civilization has resulted in an increased level of interest for enhanced requirements of safety and security, resilience and the protection of societies have become increasingly important focuses for the European Union. With the development of common assets, infrastructures, and cooperation, Europe is enhancing the security of all citizens against natural and human made risks. Horizon Europe, through Cluster 3 – Civil Security for Society continues to support the most innovative and ambitious actors of different fields, in their efforts to respond to challenges posed by many threats including natural disasters, cybercrime, and terrorism. Civil Security for Society (CL3) aims to efficiently counter the rapidly increasing security threats to the citizens of Europe. Terrorist attacks, organized crime, illegal immigration and cyber-attacks, as well as natural and man-made disasters, are putting increasing pressure on societies in Europe. In addition to technological solutions, especially against threats of an increasingly complex and digitalized society, societal and cultural behavioral patterns also evolved and must be taken in to the consideration. Ethical aspects of balancing security and freedom must also be assured in security concern. Furthermore, Europe must ensure its independence from safety-critical technologies as well.

EU-funded projects in the civil security field are crucial for enhancing the collective safety and resilience of European societies. These projects facilitate collaboration among member states, researchers, industries, and policymakers to address complex and cross-border threats. By pooling resources, expertise, and innovation, EU funding promotes the development of advanced technologies, best practices, and coordinated response strategies. These initiatives not only strengthen the EU's ability to protect its citizens but also ensure compliance with shared values, such as human rights and the rule of law, in security measures. Furthermore, they contribute to fostering trust and cooperation between member states, ensuring that Europe remains a united and secure region in an increasingly interconnected world. However, in order to develop something new, it is inevitable to understand and research what has been done and what can be improved. This document is designed with intention to highlight impactful CL3 projects with great potential uptake of project results, which can inspire, motivate, encourage future CL3 project implementors to pursue their project ideas in civil security field in order to contribute to a safer future. It also can lay the foundations for further research and innovation. This document also has an intention to show the variety of tools, instruments and environments that can be used to fight different hazards, build resilience and secure safety.

The projects that were selected for this document were either award winning projects or acknowledged by European Commission representatives highlighting them during different meetings or events.

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

Mitigating disasters with social media

Resilient society is generally known as the community or society which can withstand, absorb, adapt to, and recover from the consequences of a hazard in a timely and effective manner—including by maintaining and restoring its fundamental structures and functions. In a context of growing risks, projects funded under civil security for society field aims at securing research activities to support disaster risk management and governance through enhanced capacities, technologies and overall societal resilience. In our days the term "resilient society" is very relevant due to the increased number of natural hazards happening all over Europe as a result of global warming. In order to address various risks, including extreme weather events (floods, heat waves, storms, forest fires), geological hazards (earthquakes, tsunamis, volcanic eruptions), and slow-onset hazards (sea-level rise)—new technologies, tools, and methods are needed. Research, which results in this field is helping to lower the risks of disasters that are governed by various national, international, and EU rules.

The EU-funded project LINKS is focusing on the role of social media and crowdsourcing on disaster resilience in Europe. LINKS project has developed a scheme for understanding, assessing and managing social media and crowdsourcing for European disaster resilience. The project took into consideration the differences between disaster risk perception and vulnerability, disaster management processes and applied disaster community technologies across European communities. The project was deployed and assessed in four European countries by considering different disaster scenarios, management phases, and diverse socioeconomic and cultural environments. Five practitioner-driven European cases that represented various disaster scenarios (earthquake, flooding, industrial disaster, terrorism, drought), cut across phases of disaster management, and took place in four different countries—Denmark, Germany, Italy, and the Netherlands. Additionally, LINKS established the LINKS Community - a diverse group of stakeholders committed to enhancing European disaster resilience including first responders, government agencies, civil society organizations, business communities, citizens, and researchers throughout Europe. The LINKS Framework was developed through a practitioner-driven approach and evaluated across different countries and within specific disaster scenarios, including earthquakes, flooding, industrial disasters, terrorism and drought. The Framework can be accessed via the LINKS Community Center (LCC). Dedicated to improving European disaster resilience through the effective use of social media and crowdsourcing, the center brings together first responders, public authorities, civil society organizations, business communities, citizens and researchers from across Europe.

More information about the project: https://links-project.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/883490

A thorough communications and analytic platform was created by another EU-funded beAWARE project in order to assist citizens, first responders, and decision-makers. It consists of multilingual report generation, multilingual verbal and written communication analysis, and multimedia-enhanced emergency communication. beAWARE knowledge base is the semantic basis for the categorization scheme and deduction rules, as well as information analysis and result distribution. Local residents, first responders,

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

social media, local weather forecasts, sensors (such on site static cameras to monitor water levels) and even drone cameras are some of the sources from which information is gathered. Project goal is to add the components required to make the platforms, theories, and methodologies available at the moment in use for disaster forecasting and management function, which could effectively contribute towards the same goal. BeAWARE's primary objective is to offer assistance during every stage of an emergency situation. More precisely, it suggests an integrated solution to facilitate emergency data transmission and routing, forecasting, early warnings, aggregated analysis of multimodal data, and coordination management between first responders and authorities. As situational awareness means being able to accurately determine what has happened, what is happening now, and what will come next, all in order to plan and coordinate the most effective response possible with the resources available, beAWARE plafrom is able to offer all of it. The social media monitoring module looks for, verifies, and analyzes relevant social media content before performing spatiotemporal grouping of the postings. Moreover, through the beAWARE mobile application, citizens and first responders can communicate and get the most accurate information. Two field pilots validated beAWARE platform: a heatwave simulation in Greece, and a flood simulation in the Italian Eastern Alps region.

More information about the project: https://beaware-project.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/700475

Enhancing new technologies for securing EU borders

The objective of the European Union in the field of external border protection is to safeguard the freedom of movement within the Schengen area and to ensure efficient monitoring of people who cross both external Schengen borders, as well as the EU's external borders with countries that are not part of the Schengen area. There is a strong link between what happens outside of the EU’s borders and security within Europe. In a rapidly changing world, security challenges have become more complex and multidimensional. When it comes to security, no country should be left alone, therefore the EU made security a priority in its Global Strategy and has been working over the past years to create the conditions for Member States to collaborate more closely with each other on defense. A lot of progress has been achieved, however, more work will consolidate it.

D4FLY
DETECTING DOCUMENT FRAUD AND IDENTITY ON THE FLY

The D4FLY project aims to strengthen border authorities' capacities to combat new threats in identity and document verification at both human and highly automated border control locations, as well as in the process of issuing valid documents. From document issuance based on breeder documents, such as birth certificates, to document usage and identity verification in various border crossing scenarios, D4FLY evaluated the entire identity lifecycle. In order to improve the quality of identity and document verification and provide travelers with a seamless border crossing experience while they are on the go, the D4FLY project tools and systems looked into a variety of technologies. New algorithms and sensor technology based on sophisticated light field cameras were created to improve verification accuracy by combining the use of several biometric modalities, while performing under real-time constraints. In addition to helping to analyze and identify fraud in breeding documents, D4FLY developed a document verification system that can validate a wide range of physical and electronic security elements in travel documents, such as passports. A border

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union’s Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

control kiosk equipped with improved enrolment, verification, and detection capabilities as well as a continuous on-the-go biometric verification corridor were among the D4FLY achievements. Every innovation was examined in light of relevant laws, privacy laws, fundamental rights, and European society ideals. The project's testing and demonstration grounds consisted of four distinct border check locations and one center with expertise in document forgery. D4FLY investigated new technologies to enhance the document and identity verification process, laying the foundations for smoother border crossing experiences for travelers. Project partners collaborated with end users, gathering useful feedback on social aspects to validate the proposed technologies and better meet end user needs.

More information about the project: https://d4fly.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/833704

Another problem faced by EU border is that in recent years, there have been an upsurge in transnational crimes, especially smuggling in the Eastern EU Borders, and irregular migratory flows, which have presented the European Community with a number of issues. As a result, a comprehensive, next-generation border surveillance system is required, one that offers pre-frontier situational awareness to help relevant authorities decide on border control and response operations with more knowledge. Through the demonstration of a completely operational border monitoring system, NESTOR project decided to address all these issues. In accordance with the principles of the European Integrated Border Management, NESTOR established a fully operational, next-generation, comprehensive, and deployable border surveillance system that offers pre-frontier situational awareness beyond land and maritime borders. Factory integration tests were conducted using the Full System Operational Testing using several configurations for each trial configuration. Every NESTOR component created during the project was taken into account during the integration phase. Adequate system deployment was ensured by the system maintenance and deployment in testing settings, taking into account the use of each hardware and software system for each trial set. Moreover, project team made every effort to adhere to a modular strategy in order to minimize costs associated with system implementation and maintenance. NESTOR accomplished to improve situational awareness and pre-frontier intelligence at EU external borders by creating and integrating surveillance technologies, testing and validating them in actual international trial scenarios, and thereby enhancing European citizens' sense of security and safety. Also, by integrating the NESTOR system on top of current cutting-edge systems and infrastructures, it is possible to enable significant cost savings, performance enhancements, and speedy solution adoption.

More information about the project: https://nestor-project.eu

Information on CORDIS: https://cordis.europa.eu/project/id/101021851

Using augmented reality in fighting crime and terrorism

To keep one step ahead of criminals and terrorists, law enforcement agencies in Europe must constantly undergo digital transformation, as risks to public safety grow more serious every day. The field of augmented reality (AR) has enormous promise for intelligent law enforcement and for quickly advancing the ability to create visual comprehension of intricate real-world situations. By superimposing relevant data right

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

on top of the actual environment, augmented reality technology can significantly enhance situational awareness, a crucial skill for law enforcement personnel and citizens alike. However, the processing power of currently available technologies is insufficient to provide quick, real-time scene interpretation, which is essential for responding to terrorist and criminal occurrences.

With a variety of technological components, DARLENE is intended to be an augmented reality (AR) system for Law Enforcement Agencies (LEAs) and first responders. It aims to improve human physical and mental processing capacity and to increase situational awareness and support difficult decision-making under pressure. Situational awareness is an essential ability for law enforcement and is frequently necessary for both the officers' and the community members' life and safety. As a result, LEAs must always strive to develop a situational awareness mindset. When dealing with risky scenarios like criminal and terrorist incidents, police officers can significantly benefit from integrating such a way of thinking with cutting-edge technology. Law enforcement officers often find themselves in dangerous situations, in which split-second decisions need to be made. Taking the right course of action often depends on having access to accurate situational information. With DARLENE technologies, law enforcement agencies are able to wrest control back from terrorists and criminals. This is because the technologies created a single operating picture for both on-scene staff and their command staff, based on data gathered from several sources. Officers wear artificial intelligence (AI) glasses that deliver information to support decision-making. This information informs them of what is happening in front of them but also behind them, providing more context to the situation. This allows quicker and more coordinated scenario evaluations. A significant result is the wearable, portable prototype developed for police officers, which comprises an Augmented Reality helmet and a computation unit that implements advanced Artificial Intelligence (AI) to analyse in real-time user's field of view. This prototype, entitled Wearable Edge Computing Node (WECN) based on hands-on interaction and evaluation with police officers in the planned training and piloting sessions. In a related line of research, AI methodologies have been developed for the other two computation layers of DARLENE as well, namely the cloud and the intermediate Patrol Car Edge Node (PCEN). To interconnect the different computation layers of DARLENE, research has been focussed on the development of a private 5G infrastructure, while cyber-secure mechanisms have been developed for the authentication of different computation nodes.

More information about the project: https://www.darleneproject.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/883297

Security Critical Agents (SCAs) also known as first responders require a range of competencies, knowledge and practical experience to cope with a complex civil protection and terrorist events. These challenges can range from managing large scale cyber-attacks at the strategic level in a command center to tactical firearms training undertaken by officers on the ground. First responders need a variety of skills, expertise, and real-world experience to handle complicated civil protection and terrorist incidents. Effective SCA training faces hitherto unheard-of difficulties because of the diversity, complexity, and relative rarity of scenarios. In order to train and evaluate the skills and competencies of Security Critical Agents, which include counterterrorism units, border guards, first responders (police, firefighters, ambulance

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

services, civil security agencies, and critical infrastructure operators), TARGET provided a pan-European serious gaming platform with new tools, techniques, and content. Open TARGET Platform provides extensible standards driven methods to integrate simulation techniques and AVR technology with existing SCA training equipment, which can be customizable to local languages, national legal contexts, organizational structures, established standard operational procedures and legacy IT systems. Mixed-reality experiences immerse trainees at task, tactical and strategic command levels with scenarios such as tactical firearms events, asset protection, mass demonstrations, cyber-attacks and CBRN incidents. The TARGET platform and scenarios were developed and updated during the project by the technical and end-user partners. The TARGET mixed reality platform has been developed largely from scratch in order to support the needs of security and first responder organisations. It can be used on both a cloud and local installation basis and has also been designed to support scenarios which were not foreseen during the TARGET project. In the case of the augmented reality scenarios it is also designed to be portable and easy to set up and supports the interaction with and tracking of real world objects such as simulated radiation dosimeters or simulated weapons. It uses common of the shelf hardware solutions to provide a range of diverse and rich experiences for end users.

More information about the project: http://www.target-h2020.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/653350

Holistic approach towards resilient infrastructure

Infrastructure provides critical services to communities, supporting economic functions, and serving as the first line of defense against hazards and disasters. As the intensity and frequency of hazards continue to rise, disruptions to infrastructure systems are becoming more frequent, resulting in significant economic and societal costs. Preserving critical infrastructure requires significant investment in the resilience of infrastructure systems, so they are better able to withstand shocks and effectively deal with severe weather events such as floods, droughts, and extreme temperatures. At the same time, policymakers must prioritize disaster prevention in the management of infrastructure networks, for instance through adequate maintenance, robust monitoring systems, and proper integrations with the environment. A holistic approach towards resilient infrastructure can be very beneficial as it can engage multiple disciplines or multiple perspectives in order to create solutions to problems and/or to provide tools for coping, recovery and support.

To improve the understanding of the phenomenon of liquefaction and its mitigation, researchers from several disciplines have come together to examine the effects of earthquake-induced liquefaction across Europe. Due to this, project LIQUEFACT was created in order to protect structures / infrastructures for improved resilience to earthquake-induced liquefaction disasters in a holistic approach. While structural remediation/rehabilitation of the built environment against earthquakes is a widely studied subject, the knowledge on foundation improvement to mitigate the effects of earthquakes on buildings and critical infrastructure is limited, with existing remediation techniques being very invasive and costly. An interdisciplinary team of academics was assembled by the EU-funded LIQUEFACT project to gain a better understanding of how vulnerable European communities could be more resilient to earthquake-induced

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

liquefaction events. The goal of the project team was to create mitigation strategies for ground improvements that would lessen the effects of such occurrences on the population. In order to lessen building's vulnerability and increase its resilience to future earthquake-induced liquefaction, the study team created tools that stakeholders can use to identify affordable ground mitigation solutions. LIQUEFACT project has studied the potential impacts that an earthquake induced liquefaction event could have on Europe and produced technical guidance on how to quantify the risks at a local (micro-zonation) or site-specific scale. LIQUEFACT has compiled a database of past liquefaction occurrences and integrated this with a macro-zonation map that shows the level of risk of earthquake induced liquefaction across Europe. LIQUEFACT has also developed new techniques for modelling the damage caused by an earthquake induced liquefaction event on structures and infrastructures and evaluated three ground mitigation interventions (horizontal drains, vertical drains, and induced partial saturation) to improve soil performance. LIQUEFACT has integrated all the above into a Resilience Assessment and Improvement Framework (RAIF) and software solution (the LRG) for evaluating potential mitigation interventions to improve structure/infrastructure and community resilience. Engineers, facilities managers, and legislators can now better grasp the potential effects of an earthquake-induced liquefaction event on buildings thanks to a variety of technical and commercial tools that the LIQUEFACT team developed.

More information about the project: http://www.liquefact.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/700748/reporting

Resisting, absorbing, accommodating and recovering from hazards or disasters is a difficult task that many European cities have to go through. Therefore, the SMR project consortium has created a set of tools that intends to help EU cities to achieve resilience. As cities grow bigger and become more populated, and as climate change increasingly threatens their safety, cities need to become more resilient. Traditionally, risk management approaches have been prevailing in a common case, one-disaster scenarios but fail when dealing with interconnected risks and unforeseen events. To be fully resilient, cities need systematic tools. Systematic tools are precisely what the SMR project has been providing: a set of tools co-created with cities, allowing them to build up their resilience in an effective way. Over the course of the project, the team worked closely with the cities of Glasgow, Donostia, Kristiansand, Riga, Rome, Vejle and Bristol to develop, test and finally use the project tools. These cities have not only acknowledged the value of the SMR framework, but also continue to use it to increase their resilience. European Resilience Management Guideline and the five tools that compose it, have been co-created during the project: Resilience Maturity Model (RMM), Risk Systemicity Questionnaire (RSQ), Resilience Information Portal (RP), City Resilience Dynamics Model (CRD), Resilience Building Policies tool (RBP). The implementation pilot processes have allowed a strong cooperation among the relevant stakeholders involved in City Resilience development. The pilot projects have been conducted in the cities of Glasgow, Kristiansand and Donostia - San Sebastian. SMR project has also conducted standardization activities, where additional cities, which were not part of the consortium, and representatives from other simultaneous research projects have taken part. The project has also created a network of cities committed to cooperate in order to improve their own resilience and has developed tools and standards that provide value to operationalize resilience.

More information about the project: https://smr-project.eu/home/

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

Information on CORDIS: https://cordis.europa.eu/project/id/653569

Exploiting technology and research data's potential to different threats

Law enforcement plays a critical role in maintaining law and order within communities, ensuring public safety. Behind the scenes, law enforcement officers employ a variety of tactics and strategies to combat crime effectively. The art of crime fighting encompasses a wide array of tactics and strategies employed by law enforcement agencies. Different and innovative methods allow law enforcement officers to be better equipped to combat crime effectively and safeguard the communities. It is through their dedication, skill, and constant adaptation that they continue to serve as the guardians of law and order. The incorporation of technology has fundamentally transformed how law enforcement combats criminal activities. While traditional methods of law enforcement and community vigilance remain crucial, the integration of technology into crime prevention strategies has revolutionized safety and crime detection. Law enforcement agencies are beginning to use crime prevention approaches to keep their communities safe. On the other hand, research on fighting crime and terrorism is also crucial and depends on the availability of sufficient and high-quality data. Insufficient domain-specific data is a significant obstacle, impeding the creation and application of efficient techniques, systems, and instruments.

ASGARD's sole objective was to support the technological autonomy and efficient use of technology by law enforcement agencies. ASGARD has driven progress in the processing of seized data, availability of massive amounts of data and big data solutions in an ever more connected world. Technologies transferred to end users under an open source scheme were focusing on Forensics, Intelligence and Foresight (Intelligence led prevention and anticipation). New areas of research had also been addressed. ASGARD aimed to contribute to law enforcement agency's (LEA) Technological Autonomy, by building a sustainable, long-lasting community for LEAs and the R&D industry. This community has developed, maintained, and evolved a best-of-class tool set for the extraction, fusion, exchange, and analysis of Big Data, including cyber-offence data for forensic investigation. ASGARD helped LEAs significantly increase their analytical capabilities and has driven progress in the processing of seized data, availability of massive amounts of data, and big data solutions. The essence of the new and more efficient way of collaboration consisted of adopting and adapting to the needs of EU collaborative research projects principles and best practices of the Open Source Model (e.g., open collaboration, decentralization, peer-production, and iterative and incremental full-development cycles). In addition, an additional tool Maturity Evaluation Model (and the TRL Calculator tool developed as part of it) proposes a new multidimensional approach to evaluate the maturity of the tools delivered by ASGARD that could easily be extended to other projects. Moreover, as forensics was a focus of ASGARD, both intelligence and foresight dimensions, were significantly addressed by the project. This work has led to the development of EACTDA, a very important network for the development of new technologies in fighting cybercrime.

More information about the project: https://www.asgard-project.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/700381

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

In order to support data-oriented research collaboration between law enforcement agencies, security practitioners, pertinent EU agencies, researchers, and policymakers, the EU-funded LAGO project established a reliable EU research data ecosystem. In particular, provided a reference architecture founded in transparency and decentralization. The reference design is also backed by technology solutions to assure its practical deployment and compliance with EU data protection requirements. LAGO's overarching objective was to reinvent the field of FCT data-oriented research. To further FCT research and innovation, the research community requires a reliable and secure infrastructure for exchanging and collaboratively producing big, high-quality datasets that are sufficiently realistic and domain-specific. In order to promote access to research data in the field of the fight against crime and terrorism (FCT), LAGO tackles "The Data Issue" in the FCT research landscape by suggesting the framework for the creation of a Research Data Ecosystem (RDE). The reference architecture outlined the established and verified technological, procedural, SELP, and governance building blocks that an EU FCT RDE ought to have in order to develop into a reliable, trustworthy, safe, and long-lasting method for fostering data-oriented research collaboration between relevant EU agencies, academic and industry researchers, policy makers, and regulators, as well as security practitioners and LEAs. LAGO has developed a variety of state-of-the-art technologies, all of which tackle major issues with data access in the FCT realm. A noteworthy breakthrough improves Human Attribute Segmentation by means of adaptive techniques that perform well under a variety of conditions, and raising the bar for data processing effectiveness in circumstances with restricted access that are common in FCT. In addition, using generative models to provide realistic, high-quality samples for machine learning model training under data limitations, LAGO introduces clever data generation approaches in cybersecurity to battle botnets. This strategy enhanced with an additional ground-breaking tool that detects and embeds malware in digital images using generative techniques, greatly strengthening cyber defenses against cyberterrorism. Furthermore, the project pioneers in efficiently training visual models under data scarcity and distribution challenges, utilizing a harmonious blend of self-supervised and supervised learning within a federated framework.

More information about the project: https://lago-europe.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/101073951

Securing societies by addressing societal challenges

Security technology ought to strengthen societal resilience and advance public safety. They can, however, result in power disparities and social injustice and have significant negative effects on human rights from a societal, legal, ethical, and political standpoint. Security technology research and development seldom ever involve civil society and may not take societal issues into account in their entirety. By utilizing security technology, current European research and innovation (R&I) and security policies seek to address issues that pose a threat to European society. In general, security technologies are meant to strengthen social resilience, advance public safety, and enhance security. Security technologies can have a significant impact on society, the law, ethics, the economy, and politics, but they also spark controversy. These technologies also sometimes violate human rights, perpetuate power disparities, and bolster social inequality. Social concerns may not be adequately addressed in the study and development of security technologies since civil society is rarely or only partially involved. R&I and security technologies shouldn't foster social distrust or lead to lost opportunities but rather to work together to strengthen societal resilience.

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

Through enhanced citizen and societal engagement in security R&I, the EU-funded TRANSCEND project enables individuals and their organizations to actively and creatively engage in iterative design and deployment processes. In close cooperation with local organizations, academics, the government, and business, the project created a toolkit of techniques to increase civil society participation in security research and innovation. TRANSCEND aims to be an enabler for organisations in security R&D such that they are better equipped than currently is the state to overcome barriers to citizen engagement in security research, in active and creative roles, at an early stage of the R&D process. TRANSCEND does that by taking inspiration from existing methods to engage citizens and understand societal needs and applying selected methods to ongoing security research in four security domains of CS, DRS, FCT and BM. This enables TRANSCEND to more specifically apply existing methods to the security research arena. The TRANSCEND project represents a transformative approach in the realm of security research and innovation, aiming to significantly enhance the involvement of civil society. By developing and implementing a comprehensive Toolbox and Framework, the project seeks to align technological advancements in security with societal needs and values, fostering a more inclusive, transparent, and responsive security research environment. This deliverable outlines TRANSCEND's strategic exploitation objectives, including stakeholder engagement, continuous adaptation of tools and methodologies, sustainable impact planning, policy influence, network expansion, and ongoing improvement efforts. Through these initiatives, TRANSCEND is set to maximise the exploitation potential of its outputs, with the aim of redefining the landscape of security research, ensuring that it addresses and integrates the perspectives and concerns of civil society, thus leading to more ethical, effective, and democratically grounded security solutions. In overall, TRANSCEND contributes to the uptake of effective methods for citizen and societal engagement throughout the EU, so that civil society are given a louder voice, a place at the right tables and security practitioners are motivated and equipped to enhance such participation.

More information about the project: https://transcend-project.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/101073913

Another Engage2innovate (E2i) project is investigating and addressing barriers to implement EU security research and innovation outputs, including poor engagement with end-users, stakeholders and citizens, lack of front-end research and problem framing, and ineffective innovation processes. E2i adopts a human-centered, transdisciplinary approach recognizing innovation as requiring two key elements: novelty and implementation. Social innovation is a human-centered approach to developing meaningful solutions rooted in a rich understanding of end-user contexts, so that novel ideas (inventions) are actually implemented. Researchers demonstrates and deliver the E2i Security R&I Toolbox, enabling adoption of social innovation and human-centered design approaches to engage citizens and end users in security R&I and supporting security R&I actions in framing and designing security solutions by optimizing their acceptance and adoption. By accomplishing all the goals, E2i is strongly contributing on strengthening EU security research and innovation. Through effective engagement with security policymakers, researchers,

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

and practitioners across the quadruple helix, E2i champions good practice in social innovation and human-centered design. To promote the engagement of citizens and end users, E2i also came up with a Societal Development Plan describing the current landscape of social innovation. This provides guidance on how the approach can strengthen EU security research and innovation and includes an explanatory conceptual model and practical exemplars to inspire and motivate. Finally, E2i is built on the enthusiasm and inspiration of the next generation of researchers and design thinkers through two international social innovation design challenges, showcasing new innovative thinking and solution concepts while fostering adoption of E2i outputs.

More information about the project: https://www.engage2innovate.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/101121353

Creating novel concepts to address physical and cyber threats

Physical security and cybersecurity measures have traditionally been viewed as separate efforts. However, integrating physical security and cybersecurity can improve threat detection and response capabilities, cut costs, and increase overall security posture. Cybersecurity experts and physical security professionals are concerned with risk management and stand a better chance of keeping potential bad actors out by working together. Through the adoption of the Internet of Things and Industrial Internet of Things devices, the world is becoming increasingly interconnected. This mixture of cyber-physical systems expands the attack surface, making physical and digital security essential to prevent cyber physical attacks. An integrated security approach involving physical and cybersecurity enhances protection at every level, making defenses more robust and adaptable. By combining physical and cybersecurity threats, it is possible to gain a more comprehensive understanding of potential attacks, allowing quicker response times and more effective crime mitigation. Also, integration strengthens the overall security posture, making it more resilient to evolving threats and bolstering the ability to adapt to new challenges.

7SHIELD

The 7SHIELD project aims to create a comprehensive framework that facilitates the implementation of novel services for the cyber-physical protection of ground segments. This covers laser technology, passive radars, and e-fences. In order to evaluate the prevention, detection, and mitigation of threats, both physical and cyber, the project is making use of cutting-edge technologies for data integration, processing, analytics, and visualization in addition to data security and cyberthreat protection. Five installations of space system ground segments can serve as test and demonstration sites for the project.
To better prevent, detect, respond to and mitigate threats at ground level, 7SHIELD integrates seven key technologies: IoT, high-level analytics, decision support systems, crisis management, situational awareness, semantic reasoning and sensors. 7SHIELD covers measures to be taken before, during and after a crisis. Its multilayered architecture ensures that its 32 modules work together seamlessly at each stage, from data capturing and threat detection to the creation of a global view and the triggering of appropriate responses. 7SHIELD integrates a series of cross-cutting technological achievements in each phase of the crisis management. 7SHIELD also addresses and provides solutions for security investment planning and optimization thanks to an impact assessment model which estimates the economic impact of the implementation to support the exploitation of the outcomes. By doing that 7SHIELD provides an additional layer of protection of European economy and reducing dangers to societal stability. Finally, the consortium

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

closely followed the required legal and ethical requirements compliance especially with those related to the data acquisition and use of artificial intelligence (e.g. availability of open source and online data, privacy, copyright, terms of service, video surveillance, facial recognition and wearable technologies).

More information about the project: https://www.7shield.eu/project/

Information on CORDIS: https://cordis.europa.eu/project/id/883284

PHOENIX PHOENIX aims to offer a cyber-shield armor to European EPES infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guaranteeing the continuity of operations and minimizing cascading effects on the infrastructure itself, the environment, the citizens and the end-users at reasonable cost. Europe's Electrical Power and Energy System (EPES) is one of the most complex cyber-physical systems in the world. Any attacks bringing down this critical infrastructure could have a vast cascading effect on others, including water supply, communications, transportation, industry and finance. In the EU-funded PHOENIX project, researchers developed a cyber-shield security platform for European EPES infrastructure, enabling it to detect and survive large-scale, combined cyber and privacy attacks at a reasonable cost. The PHOENIX project had three major goals. The first was to strengthen EPES cyber defense by designing novel protective concepts for resilience, survivability, self-healing and accountability to be used within Europe's infrastructure. The PHOENIX team also innovated existing systems, adapting, upgrading and integrating a number of tools and validating them in large-scale pilots. The second goal was to improve coordination between European EPES cyber incident discovery, response and recovery. To do this, PHOENIX members created a fully decentralized cybersecurity information awareness platform for authorized stakeholders across Europe. The third initiative was to accelerate research and innovation within EPES cybersecurity. The PHOENIX team established a series of certification methods and procedures through a newly created Cybersecurity Certification Centre. The PHOENIX security platform monitors for new incidents and identifies and mitigates against attacks. PHOENIX generated increased awareness of cyberattacks among stakeholders in European EPES, which resulted in fewer service disruptions due to incidents being detected earlier. Other tools developed during the project include the 'Secure, Persistent Communications (SPC)' platform, a cloud-based communications layer which ensures all data are legitimate and secured. The Privacy Protection Enforcement (PPE) toolkit uses consent-based approaches to evaluate and mitigate risks associated with identified attacks.

More information about the project: https://phoenix-h2020.eu/

Information on CORDIS: https://cordis.europa.eu/project/id/832989

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

Conclusion

Civil security is essential for ensuring the safety and well-being of individuals, communities, and nations. It encompasses measures to protect citizens from threats such as natural disasters, terrorism, cyberattacks, and public health emergencies. By maintaining robust civil security, governments and organizations can prevent loss of life, minimize damage to infrastructure, and foster societal resilience in the face of crises. Effective civil security also promotes trust in institutions, supports economic stability, and safeguards democratic processes. Ultimately, it underpins a secure environment where individuals can thrive, contributing to the overall progress and stability of society.

Modern, multicultural countries face challenges in all areas of life related to civil security. It enhances the establishment of democratic societies where social cohesion and societal involvement are prioritized and allows citizens to grow freely and autonomously. Civil security research needs to adapt in response to shifting security policy environments, the growing tendency toward digital technology in both personal and professional spheres, and societal change. Comprehensive solutions that address the effects of organized crime and international terrorism as well as improving the security of vital supply infrastructures must be a part of this approach. In addition, action at both the national and international levels is required to lessen the effects of extreme weather events and natural disasters. Organizations involved in public and private safety and security face significant, sometimes novel issues in the area of civil security.

Projects in civil security field bring professionals of different countries around the same table for a constructive dialogue. They come from all levels – from research, governmental, business representatives to fire fighters and police officers. The goal is always to build trust and long-term working relationships and create a network of professionals, working together on innovations who would not hesitate to contact each other when a crisis comes. The essence and the main purpose of cooperation in the area of civil security is building a common societal security culture**.** It is important to build common attitudes towards societal security threats and a shared understanding of prevention, preparedness, and response as well as recovery processes in connection with disasters. A broad, whole-of-society approach and cooperation, readiness to act jointly and shared know-how are important components of effective crisis management whenever disasters or accidents occur.

EU-funded projects in the civil security field are crucial for enhancing the collective safety and resilience of European societies. These projects facilitate collaboration among member states, researchers, industries, and policymakers to address complex and cross-border threats. By pooling resources, expertise, and innovation, EU funding promotes the development of advanced technologies, best practices, and coordinated response strategies. These initiatives not only strengthen the EU's ability to protect its citizens but also ensure compliance with shared values, such as human rights and the rule of law, in security measures. Furthermore, they contribute to fostering trust and cooperation between member states, ensuring that Europe remains a united and secure region in an increasingly interconnected world.

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472

References

https://cordis.europa.eu/projects/en

https://links-project.eu/

https://beaware-project.eu/

https://d4fly.eu/

https://nestor-project.eu

https://www.darleneproject.eu/

http://www.target-h2020.eu/

http://www.liquefact.eu/

https://smr-project.eu/home/

https://www.asgard-project.eu/

https://lago-europe.eu/

https://transcend-project.eu/

https://www.engage2innovate.eu/

https://www.7shield.eu/project/

https://phoenix-h2020.eu/

SEREN5 (SEcurity REsearch NCP Network 5) has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement number 101073472