SECURIT

TOWARDS RESILIENT SMART CITIES & TERRITORIES

Project Deliverable

D4.4 Gap Analysis & Repository Reference Document of Security and Cybersecurity Requirements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Deliverable information	
Grant Agreement	N°101005292
Project Acronym	SecurIT
Project Title	New industrial value chain for Safe, sECure and Resilient clties and Territories. Call: H2020-INNOSUP-2020-01-two-stage - Cluster facilitated projects for new industrial value chains
Type of action	Supporting and co-financing the development of collaborative projects
Revision	V1
Due date	31/08/2024
Submission date	31/08/2024

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission)	
RE	Restricted to a group defined by the consortium (including the Commission)	
CO	Confidential, only for members of the consortium (including the Commission)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Version	Date	Document history	Stage	Distribution
V0.1	18.10.2022	Document Creation	Draft	LSEC + partners
V0.2	18.10.2023	Document Revision	Draft	LSEC + partners
V0.3	20.01.2024	Document Revision on basis of 2nd Open Call	Draft	LSEC + partners
V0.4	20.04.2024	Document Revision on basis of research analysis + contribution of partners	Draft	LSEC + partners
V0.95	21.07.2024	Document Revision on basis of market study analysis (CIMA) and additions	Draft	LSEC + partners
V1.0	21.08.2024	Final revision and review	Final	LSEC + partners

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table of content

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

LIST OF TABLES AND FIGURES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

ABSTRACT

SecurIT is a project with a **market-pull orientation**, that has aimed at funding **innovative SME solutions** in the security area that address common gaps and needs identified by security practitioners.

The four year project has been successfully leading two Open Calls, and supporting over 40 companies in their innovations and going to market activities. The Open Calls have learned the SecurIT consortium what innovative technology companies in the domain of critical infrastructure protection, physical security and cybersecurity amongst other are currently working on in terms of innovations, market challenges and user requirements. The project has successfully supported these innovations to be demonstrated by the respective Open Call applicants or proven the concept of the anticipated ideas and targets. These results have been validated throughout the lifetime of the Open Call projects (12 months). Some of the results of the Open Call 1 and Open Call projects have now entered into a go-to-market stage, responding to customer demand. These products and services are now commercially available and demand is growing. Others are continuing to further discuss going from demonstrator implementation into production. A third category will continue developing further on the product or service, searching for the right product-market-fit, which in many cases is behind the corner. A final group is continuing its research endeavours, or implementing products and services with the financing of the EC (through the DEP-program) or additional research funding (Horizon, regional funding, …). Some of the participating companies have realised investment rounds, and will continue to finance their additional developments with private equity funding.

This document has been performing a Gap Analysis & Repository Reference Document of Security and Cybersecurity Requirements. It is one of the concluding documents and future-forward looking document of the SecurIT project. It was planned for to be delivered on M36 of the project, the very last month – aiming to collect and report about the overall results of the analysis and open calls and to further provide the right context on the positioning of these applications and the developing demands.

This deliverable D4.4 draws on results from the challenge definition Tasks 2.1 to 2.3, the Open Call results from Tasks 3.1 to 3.4, Task 4.4 Gap analysis and relevant external sources. The report brings together the results of SecurIT work (Section 2) to:

- Identify EU Security and Cybersecurity **market gaps**, common gaps and needs identified by security practitioners that offer **opportunities for SME innovations** and address security threats to citizens;
- Analyse the SME solutions (products/services/expertise) offered in Cluster ecosystems to examine **market fit**, **technological focus** and their **security functions**;
- Analyse **regional strengths and weaknesses** including **barriers to SME innovation** and **methods to help SMEs address the barriers;**
- Analyse the Open Call bids by SMEs into the SecurIT Open Calls, to see **how well SME proposals matched the user needs in practice.**
- Identify **potential gaps between supply and demand** highlighted by SecurIT results.

The report then combines SecurIT results with results of other EU supported policy development activities covering Cybersecurity, Critical Infrastructure Protection (CIP), Disaster Resilient Societies (DRS) and the Fight against Crime and Terrorism (FCT) in Section 3 to identify **Cross-cutting Technology Development Gaps/ Needs**, providing opportunities for SMEs. Section 4 presents overall Conclusions and Recommendations.

Key Deliverable outputs are:

- **The SecurIT Repository of Security and Cybersecurity Requirements** that presents common gaps and needs identified by security practitioners for the **Sensitive Infrastructure Protection, Disaster Resilience and Public Space Protection (Major Events)** domains in SecurIT and that offer opportunities for SME innovations and address security threats to citizens.
- **Identification of fifteen Cross-cutting Technology Development Gaps/ Needs** from the results of SecurIT and other EU supported policy development projects with wider relevance across the **Cybersecurity, Critical**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Infrastructure Protection, Disaster Resilient Societies and the Fight against Crime and Terrorism domains where innovation is needed, providing opportunities for SMEs.

Recommendations are:

1) It is recommended that the **SecurIT Repository of Security and Cybersecurity Requirements** is used by policy makers to guide future EU calls for innovation proposals in **Sensitive Infrastructure Protection, Disaster Resilience and Public Space Protection (Major Events)**.

2) It is recommended that consideration is given to developing a **pan-EU online funding tool** to make it easier for SMEs to access funding instruments at regional, national and EU level and help SMEs to scale their security solutions.

3) It is recommended that the **fifteen Cross-cutting Technology Development Gaps/ Needs** identified from the results of SecurIT and other EU supported policy development projects, covering the **Cybersecurity, Critical Infrastructure Protection, Disaster Resilient Societies and Fight against Crime and Terrorism domains**, are considered as SME innovation topics for research agendas by EU policy makers.

4) It is recommended that EU policy makers consider using a **project clustering approach** to enable SMEs (with solutions or components of solutions to counter emerging technology threats) to interact with end-users (from different domains and MS with access to funding), to help **accelerate adoption of SME solutions to address emerging technology threats**.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Authors (organisation)

LSEC, SAFE, SCS, L3CE.

Reviewers (organisation)

All Partners.

Keywords

Cyber Physical Security, Cybersecurity, Sensitive Infrastructure Protection, Disaster Resilience, Public Spaces Protection, Access Control, Command and Control, Communications, Data Protection, Post Event Recovery, Warning Systems.

Legal notice

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Deliverable D4.4 Gap Analysis & Repository Reference Document of Security and Cybersecurity requirements

This Deliverable presents the Repository Reference Document of Security and Cybersecurity requirements. It identifies EU Security and Cybersecurity market gaps, common gaps and needs identified by security practitioners that offer opportunities for SME innovations and address security threats to citizens; analyses how well SME solutions offered to SecurIT match the user needs; analyses regional strengths and weaknesses including barriers to SME innovation and methods to help SMEs address the barriers; and combines SecurIT results with results of other EU supported policy development activities in the SecurIT domains to identify Cross-cutting Technology Development Gaps/ Needs that offer a potentially attractive business case for SMEs. Conclusions and Recommendations are presented.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

1. INTRODUCTION AND APPROACH

1.1 Introduction

The Security and Cybersecurity market is characterised by the following challenges which have a strong impact on SMEs:

- On the demand side:
  - high-end security equipment characterised by a relatively restricted number of customers,
  - fragmented, market segments;
  - lack of awareness: leading to 'inappropriate' procurement decisions.
- On the supply side:
  - lack of awareness: Supplier perceive that there is insufficient clarity on the expectations and requirements of users;
  - lack of experimentation: the innovation is driven by the capacity to experiment in real condition.
- Privacy and ethics:
  - rules are a strong constraint for testing and experimental solutions, in particular, those which manage personal data.
- Performance standards:
  - often performance standards are not clearly defined, or differ [unnecessarily] across market segments;
  - the absence, or difference, of technical standards across market segments results problems of interoperability and contributes to market fragmentation
- Certification systems:
  - the slow overall speed at which approval/certification process can mean that technologies are already outdated before they receive approval.

SecurIT is a project with a **market-pull orientation**, that has aimed at funding **innovative SME solutions** in the security area that address common gaps and needs identified by security practitioners. In order to give the priority to the most promising innovations and solutions, aiming at resolving or preventing a serious security threat for territories and cities, the consortium implemented two cycles of consultations to give the floor to security practitioners and permitted them to express needs, and discuss priorities towards safer and more secure cities and territories. All the processes and the methodology followed are contained in deliverables *D2.1 SecurIT challenges definition linked to Open Call 1* and *D2.2 SecurIT challenges definition linked to Open Call 2*.

The project has provided **funding to consortia of EU SMEs** offering innovative security solutions to develop prototypes and demonstrators, selected through two Open Calls whose requirements address needs identified by security practitioners. The results of the Open Calls are described in Deliverable *D3.3 Open Call Outcome report (Month 10 and Month 22).*

An online interactive mapping capability for security solutions proposed in SecurIT has been developed in the framework of the SecurIT project, presenting solutions that are applicable to the SecurIT domains and challenges. These security solutions have been identified by SecurIT cluster partners and ambassador clusters, based on the products/services/expertise provided by the companies of their ecosystem, and have also been proposed directly by developers of technological solutions. The solutions proposed have been captured by the consortium in the publicly available **SecurIT mapping platform Securit-project.eu**, designed to help users with needs and supply chain partners including SMEs with innovative solutions to connect and collaborate. The platform and mapping process is described in deliverables *D2.3 Cybersecurity and security sector offers analysis 1 - Mapping of security solutions offers* and *D2.4 Cybersecurity and security sector offers analysis 2 - Mapping of security solutions offers)*.

SecurIT has also carried out an **analysis of European Structural and Investment Funds (ESIF)** and aligned them with a portfolio of funded SMEs. The project has also analysed the success of SME support measures and identified **barriers and challenges that SME's face** developing offerings in the security sector, and **methods to help SMEs address the barriers**, described in detail in deliverable *D2.5 Synergy analysis with ESIF*.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

1.2 Approach

This deliverable D4.4 draws on results from the challenge definition Tasks 2.1 to 2.3, the Open Call results from Tasks 3.1 to 3.4, Task 4.4 Gap analysis and relevant external sources. The report brings together the results of SecurIT work (Section 2) to:

- Identify EU Security and Cybersecurity **market gaps**, common gaps and needs identified by security practitioners that offer **opportunities for SME innovations** and address security threats to citizens;
- Analyse the SME solutions (products/services/expertise) offered in Cluster ecosystems to examine **market fit**, **technological focus** and their **security functions**;
- Analyse **regional strengths and weaknesses** including **barriers to SME innovation** and **methods to help SMEs address the barriers**;
- Analyse the Open Call bids by SMEs into the SecurIT Open Calls, to see **how well SME proposals matched the user needs in practice.**
- Identify **potential gaps between supply and demand** highlighted by SecurIT results.

The report then combines SecurIT results with results of other EU supported policy development activities covering Cybersecurity, Critical Infrastructure Protection, Disaster Resilient Societies and the Fight against Crime and Terrorism (Section 3) to identify **Cross-cutting Technology Development Gaps/ Needs** with relevance across these domains where innovation is needed, providing opportunities for SMEs.

Section 4 presents overall Conclusions and Recommendations.

The following **types of gaps** between SME innovation supply and demand have been considered in this work:

- Market
  - Customer Needs not met by existing products and services
    - Requires development of new and unique products or services that haven't previously existed, which may require new capabilities, new technologies etc.
- Supply
  - Capability
    - Gaps in capability (e.g. equipment, facilities, tools) to provide technologies, products and services to meet current and future customer needs
  - Technology development
    - Areas where technical improvement/ technology R&D is needed to meet cybersecurity and security performance objectives
  - Technology Transfer and Uptake
    - Readiness of System Integrators and suppliers to adopt new technologies from SMEs (licensing, procurement, purchase of company etc)
  - Skills
  - User Interface/ Usability (UX)
    - Ease of interaction with cybersecurity and security technology
  - Access to Investment for SMEs
    - Public Investment
    - Private Investment (Investor views e.g. from VCs)
- User Acceptance
  - Readiness of Users to adopt innovations from SMEs (Early and late adopters).
  - User Interface/ Usability (UX)
    - Ease of interaction with cybersecurity and security technology
- Societal
  - Cross-cutting enablers and blockers e.g. societal norms and acceptance.

Target audiences for the report are:

- European Research agenda leads (EC, NCP's);
- European Cybersecurity Competence Centre & Network/ National Coordination Centres (NCCs);
- EU Policy Makers and National Strategic Agenda Policy Makers;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

- Communities of Users for Security and Cybersecurity;
- Regional and National Research Agenda leads (public investment) and Investors (private investment).

1.3 GAP analysis methodologies

Different methodologies were used the for the repository reference and gap analysis.

- End user interviews & interactions
  - Early on in the project (M3) the SecurIT project organised a series of workshops engaging end users from critical infrastructure, security services organisations and law enforcement to consider the proposed domains for innovative developments, in order to steer the Open Calls – specifying the demand.
- SecurIT catalogue gap analysis
  - The SecurIT published and online catalogues represent already a repository reference of Security and Cybersecurity
  - Analysis was done on the available offerings from the various solutions providers, versus demand side from industry market analysis and offerings from non-European providers
- SecurIT Open Call 1 and 2 gap analysis
  - The results of the Open Calls, both in terms of applications and final selections, was a source for additional insights in the gap analysis
  - Compairison was made between Open Call 1 and 2, in terms of solutions developed and innovations under development
  - Compairison was made on the domains and topics of the ones applying versus the ones finally selected and executed during the Open Call project executions
- Research of identified gaps for security and cybersecurity
  - Analysis of existing research and results from other projects and used as baseline for identifying gaps
  - Analysis and collection of gap analysis of European collaborative projects and research
- Inputs from the SecurIT discussions on gaps
  - Interactions with the SecurIT partners during bi-monthly WP4 meeting and mentoring analysis
  - Interactions and mentoring of the SecurIT Open Call participant representatives, during presentations on the SecurIT closing conference, and during mentoring meetings
- Research and Analysis of the Cybersecurity Industry Market Analysis (CIMA) 2024
  - Analysis of research results and identification of gaps of CIMA 2024 (not yet published)
  - Gap-analysis of data sets with market data, product categorization and actual

The resulting analysis has been compiled into this report.

2. SecurIT Challenges Definition and Open Call Results

2.1 Introduction

The SecurIT project aimed at supporting innovative technological solutions in the field of security, developed by consortia of European SMEs, that were granted a prototype or demonstrator project, through a top-notch selective process of two Open Calls. The project support collaborative projects supporting a new industrial value chain.

A total of 21 projects were funded during the Open Call 1, based on two instruments that is 7 prototyping projects with a maximum budget of 74.000 euro and 14 demonstrations projects with a maximum budget of 88.000 euro. An additional 21 projects were funded during the Open Call 2 (OC2), based on the two instruments, again 7 prototyping projects with a maximum budget of 74.000 euro and 14 demonstrations projects with a maximum budget of 88.000 euro. The projects were selected based on a rigorous screening and selection process described in deliverable D3.6 “Open Call Outcome report and Open Call Evaluation report 2”.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

In addition, for the OC2 projects, it turned out during the economic eligibility screening process, that two SMEs in two different projects consortia were not eligible to obtain financial funding. Despite not received cascade funding, the afflicted companies decided to stay in the project consortium and remained actively involved during the project period.

This Section describes the process used to generate user needs and presents the resulting repository of security and cybersecurity requirements (Section 2.2), analyses how the SME security solutions offers from partner clusters captured on the SecurIT online platform to support collaboration match SecurIT user needs and the functions they provide (Section 2.3), studies regional strengths and weaknesses in relation to SME innovation (Section 2.4), analyses the Open Call results (Section 2.5), and draws conclusions (Section 2.6).

2.2 User Needs Analysis and Repository of Security and Cybersecurity Requirements

The EU-project SecurIT aims at providing funding to consortia of EU SMEs offering innovative security solutions in order to develop prototypes and demonstrators, and selected through two Open Calls,

The project organised workshops before each open call's launching, reuniting end-users and integrators of security solutions to help structuring the use cases and scenarios that will be addressed by the SMEs projects.

These challenges were defined through the work carried out in WP2, related to SecurIT Challenges definition, via the lead of L3CE, as WP2 Leader. The objective of Task 2.1. Needs analysis and expression of security solutions integrators and end-users led by SAFE was to obtain a clear definition of the challenges to be addressed in SecurIT project. The work was carried out through an extensive process of consultations of +35 end-users and integrators reunited in thematic workshops that conveyed their challenges to be tackled and expressed their expectations for solutions to be provided from small and medium European companies.

The second process that was conducted in the second cycle of the project, in order to update the list of challenges that were showcased in the 1st Open Call launched in January 2022. These challenges are defined through the work carried out in WP2, related to SecurIT Challenges definition, via the lead of partner L3CE - WP Leader. The objective of Task 2.1. Needs analysis and expression of security solutions integrators and end-users led by SAFE was to obtain a clear definition of the challenges to be addressed in SecurIT project. The work was carried out through a consultation process gathering security experts, to discuss the current gaps and needs in the market.

Upon the start of the SecurIT project, the consortium early launched a process of consultations at the end of November 2021, that consisted in holding three two-hour workshops, reuniting around the table end-users and integrators, that had been invited by each consortium's members. Due to the travel restrictions and the time-constraints, the consortium opted for online meetings, in lieu of physical events. The aim of these workshops was to define the needs of integrators and end-users in terms of security for the 1st Open Call. The ultimate expected result was to design a tailored-made call for propositions, suitable for end-users and integrators that had identified the common gaps in security, to be tackled. These challenges are to be inserted in the Guide for Applicants of Open Call 1 (cf. deliverable D3.1), and on the website of the SecurIT project. The 3 workshops took place on November 18 and 19th 2021, two months prior the opening of Open Call 1, and the invitations were launched at the end of October 2021.

It is a project with a market-pull orientation, aiming at funding innovative solutions in the security area that address common gaps and needs identified by security practitioners. In order to give the priority to the most promising innovations and solutions, aiming at resolving or preventing a serious security threat for territories and cities, the consortium implemented two cycles of consultations to give the floor to security practitioners and permitted them to express needs, and discuss priorities towards safer and more secure cities and territories.

As part of the project's activities, these consultations took place within the Work package 2 Task 2.1, dedicated to the definition of the SecurIT challenges that would later be presented to the technology providers. SAFE led the process with the support of the consortium members. The objective of this action was to identify common gaps, which later turned into the basis for the calls' description. It allowed SecurIT partners to propose strategic challenges in a cross-border and cross-sectorial industry value chain, that ensured a real interest for SMEs

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

responding to the Open Calls, in terms of the potential expected market as well as the business and collaborations that could be developed, while matching current and future needs of practitioners.

The activity was carried out from the start of the project, and SAFE organised several discussions around 3 topics the consortium identified in a first phase: *Domain #1: Sensitive infrastructure protection, Domain #2: Disaster resilience, Domain #3: Public spaces protection – major events*, gathering over 35 key experts in the field, end-users, LEAs, and integrators. During these dedicated workshops, participants were asked to specify and share their actual and future needs in terms of security solutions, and expressed their expectations for solutions to be provided from small and medium European companies. Several categories of security challenges had been pre-defined: a first list of challenges, segmented in 3 main domains, had been prepared and agreed among the consortium prior to the workshops, in order to have the most representative security challenges presented as a point of departure.The results of the workshops were then synthesized and turned into revised tables of challenges that were the core of the Open Calls. The challenges were captured in a table with sub-domains and 11 challenges and potential areas of needs, segmented according to technologies.

At the end of the selection process of the 1st Open Call, it was found out that two thirds of the 111 applications received targeted the 1st domain on protection of critical infrastructure, while the rest of applications were equally split between the two other domains:

- Domain 1: 67 applications and 14 selected projects for funding in this area
- Domain 2: 22 applications and 3 selected projects for funding in this area
- Domain 3: 22 applications and 4 selected projects for funding in this area

In order to improve the methodology for the Open Call 2 and to learn from past lessons, the SecurIT consortium analysed the results of the first selection process. It was decided to update the challenges, to make them more precise, merge them if needed, and encourage proposals to address challenges that had been less well addressed in Open Call 1. The consortium involved the Advisory Board members and implemented their contributions and ideas in order to update and reshape the challenges of the call for Open Call 2.

The Open Call 2's vision was guided by 3 key points:

- SecurIT focuses on digital applications to resolve security challenges
- Some challenges of Open Call 1 were not addressed by applicants
- The overall objective is to find the best fit to address market gaps.

The following questions were posed to security end-users and practitioners in order to launch the Open Call 2 discussions:

- What are your main gaps in terms of security?
- What are your main needs in terms of security? /needs perceived from the security market?
- What type of digital applications would you expect? (focusing on digital innovative solutions)
- How could the challenges of the 1st open call could be rephrased or amended?
- What other challenges could be added/ what other need have you identified?
- Would you provide any test beds?
- How you find these challenges relevant to security market (with a score for each challenge?)?

The discussions and inputs provided by the experts permitted the consortium to redefine the challenges in a better and more precise way, while keeping the 11 challenges and 3 domains. Inputs from the Deloitte/ Ecorys EC Security Market Study (May 2022) were also used to fine-tune the challenges, following the priorities of the European Commission in terms of security segmentation: resilience of critical infrastructures, disaster resilient societies, border management and fighting counter terrorism.

Open Call 1 user needs analysis results :

More than 35 end-users and integrators of security solutions have conveyed their challenges to the SecurIT project and its partners through dedicated workshops. In these workshops, they expressed their expectations for solutions to be provided from consortiums of small and medium sized European companies. Those SMEs will have the opportunity to get direct financial support from the SecurIT project to develop their solutions through individual vouchers up to €60,000 and access to a wide range of tailored professional services.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

- Domain #1: sensitive infrastructure protection

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #1: sensitive infrastructure protection	Cybersecurity	1	Development of cybersecurity solutions for sensitive infrastructure protection	To propose effective solutions for: - Cybersecurity of information and communication systems; Data protection; electromagnetic protection; - Cyber Security incident management; - Cybersecurity - Automatic attack detection and remediation; - Quantum - Post Quantum; - Security Bill of Materials - Device - IoT Security - Shared Responsibility; - Secure Sovereign Cloud.
	Operations	2	Optimisation of communication networks and alert systems	To optimize solutions for better communication networks (assess, detect and alert both operational forces, LEA or emergency services), the hyper vision and command systems and alert systems.
	Identification and access control	3	Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk.	To propose innovative solutions to identify, provide entry for and inspect individuals, vehicles and goods requesting access to the site such as: - Access control for people; - Biometrics & multi biometric systems; - Vehicle control & inspection; - Detecting weapons & explosives: stationary or mobile illicit materials like CBRNE (chemical, biological, radiological, nuclear and explosives) and weapons.
	Zone security and perimeter protection	4	Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions	To propose innovative solutions such as: - Data sensors: detectors; system status indicators; IoT; - Video analysis & sensor fusion: deep learning; - Surveillance – Essential components of the decision-making chain are the detection, recognition and identification of land/air/sea vessels and intruders near or inside the protected area – e.g.: optronic solutions; radar sensors; solutions and data processing/analysis software; video protection (embedded AI); - Surveillance Robots: patrol rounds and missions - detection/identification/neutralization of malicious drone; - Securing physical access routes through digital solutions.

Considerations following OC1 and leading to OC2 on basis of the Advisory Board (see later) :

The solutions developed in this domain will have to integrate the following considerations: maintainability, acceptable price, foresight scanning, and interoperability with existing solutions.

- Domain #2 - Disaster resilience

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #2 - Disaster resilience	Prior to crisis – prediction: Risk knowledge and evaluation	5	Optimisation of prediction of disaster	To propose innovative solutions to: - Enhance exploitation of monitoring data and satellite/remote sensing information as well as artificial intelligence to improve high-level assessment - Production and processing of data by satellite and aerial imagery (UAV/UAS and light aircraft), as well as by sensor networks. This allows for knowledge about areas concerned and potential risks, integrating data about weather and water courses, providing operational maps for decision-makers and rescue managers. - Modelling and geographical information systems: Modelling territories and the simulation of phenomena allow for the substitution of rarely accessible situations by virtual situations in realistic and operational 3D.
	During the crisis: Communication and warning systems	6	Optimisation of communication and warning systems in case of disaster	These communication systems must be easily transportable and easily deployable within a timeframe compatible with operational demands. The requirement is to have means of communication, which are suitable, diversified, and interoperable such as: - Technology that enables the management and monitoring of communication from news media, social media, and internal communication sources in a crisis situation - Information vs decision with the support of AI To propose innovative solutions to improve forecast / early warning systems, advanced data management, Information update.
	After the crisis: Post event analysis and recovery	7	Development of solutions for a better recovery	To propose innovation solutions, post crisis and recovery: • Robotics to carry out tasks in hazardous areas for humans • UAV/UAS can view an « area of interest » and give a good understanding of the environment and the situation in the area affected by a disaster • Energy and data network rehability, autonomous and decentralized – to ensure the conservation of the security of data in the context of post-disaster.

Considerations following OC1 and leading to OC2 on basis of the Advisory Board (see later) :

The solutions developed under this domain will have to consider citizen involvement and acceptation and transparency. All solutions will also have to ensure the continuity of operations.

- Domain 3 : public spaces protection – major events

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #3 - Public spaces protection – major events	Detection and alert	8	Gather and manage real time information	To propose innovative solutions to gather and manage real time information such as facial and vehicle recognition; CCTVS & cameras (eg: embedded AI for flow detection and crowd surveillance, smart cameras, etc.), signal jamming devices for drones, wave scanners systems and anomaly detection systems. To propose warning systems such as innovative tools for public and/or geolocation of public and rescue team.
	Analysis	9	Analyse and extract pertinent and potentially crucial information as quickly as possible	To propose innovative tools that can be used in real-time mode (alert, surveillance, or intervention) or in delayed mode (intelligence, investigations, e.g.: audio analytics systems, SOP updates, blind-spot mapping, performance analyses and determining training programmes etc.). To propose innovative analysis tools to support the responsible authorities in monitoring the public information space and quickly identifying disinformation threats
	Command and control (resource management) and decision- making support	10	Communication networks and post - event analysis	To produce innovative safe tools that support event planning and resource management during the event. Such tool should support: - connectivity of different authentication level users; - definition of environment (defining time, uploading geo information, defining roles, etc.); - possibility to see location of resources and communicate with all linked entities directly via safe tool; - possibility to provide visual guidance; - possibility to upload new relevant data and share with respective entities; — possibility to manage few events at a time. To propose innovative solutions for better communication networks, post event analysis

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Data protection and cybersecurity – cybercrime	11	Detection

To propose innovation solutions such as:

- AI manipulated content analysis: deep fake video detection; deep fake audio detection
- Methods for identifying information sources / provenance of information: detection of similar information appearing in different venues / platforms; attribution of information to a single source
- Media forensics: image forensics (content manipulation detection; copy-move, splicing, inpainting, enhancement)
- Video forensics (content manipulation detection; traditional cut, delete, paste attacks, copy-move, splicing, inpainting, enhancement); audio forensics (content manipulation detection, traditional cut, delete, paste attacks)
- Textual content analysis: Image content analysis; Audio content analysis; Video content analysis
- Security bills of materials device IoT security shared responsibility

Considerations following OC1 and leading to OC2 on basis of the Advisory Board (see later) :

The solutions developed in this domain will have to consider the legal constraints of personal data protection.

The process used for the definition of the challenges for the Open Call 2 was slightly revised compared to the 1st cycle. The consultations previously held at the start of the project in M3 gathered needs and gaps from a great number of end-users and integrators, which were consolidated into 3 main domains and 11 related-challenges for Open Call 1.

An Advisory Board was established at the start of the project, composed of 7 members and experts on the security field, from various countries. The Advisory Board held a first meeting at M6 of the project, and the coordination entity of this expert group, L3CE, would organise 2 meetings a year. They were invited to the 1st Jury day that took place at the end of June 2022 in Paris (M10) but due to agenda constraint, they could not attend the pitching session of the pre-selected candidates. When the selection process of Open Call 1 was achieved, they informed and granted access to the description of funded projects under Open Call 1.

Annex 2 presents the final version of the challenges as used in Open Call 2, the Repository of Security and Cybersecurity Requirements produced by SecurIT.

All the processes and the methodology followed are contained in deliverables *D2.1 SecurIT challenges definition linked to Open Call 1* and *D2.2 SecurIT challenges definition linked to Open Call 2*.

The published SecurIT Repository of Security and Cybersecurity Requirements presents common gaps and needs identified by security practitioners for the Sensitive Infrastructure Protection, Disaster Resilience and Public Space Protection (Major Events) domains that offer opportunities for SME innovations and address security threats to citizens.

2.3 Mapping of Security Solutions Offers and SecurIT Mapping Platform

As part of Task 2.2, an online interactive mapping capability for security solutions proposed in SecurIT has been developed in the framework of the SecurIT project, presenting solutions that are applicable to the SecurIT domains (3) and challenges (11).

Those security solutions have been identified by SecurIT cluster partners and ambassador clusters, based on the products/services/expertise provided by the companies of their ecosystem, and have also been proposed directly by developers of technological solutions.

The identified solutions proposed by companies (mainly SMEs), have been classified according to the SecurIT domains and challenges defined in Section 2.2 in terms of use cases and applications to examine **market fit**, and also according to their **technological focus** and their **security functions**. The solution types (functions) are defined as follows in three main areas:

Cybersecurity - according to ECSO taxonomy:

- Identify
- Protect
- Detect

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

- Respond
- Recover

Cyber-physical security services:

- Audit, planning and advisory services (e.g.: Security audit, vulnerability and intrusion testing, and risk and threat assessment)
- System integration and implementation services (e.g.: Implementation and integration, interoperability testing)
- Management and operations services (e.g.: Security system management and operations)
- Security training services (e.g.: IT / cyber-security education and training)

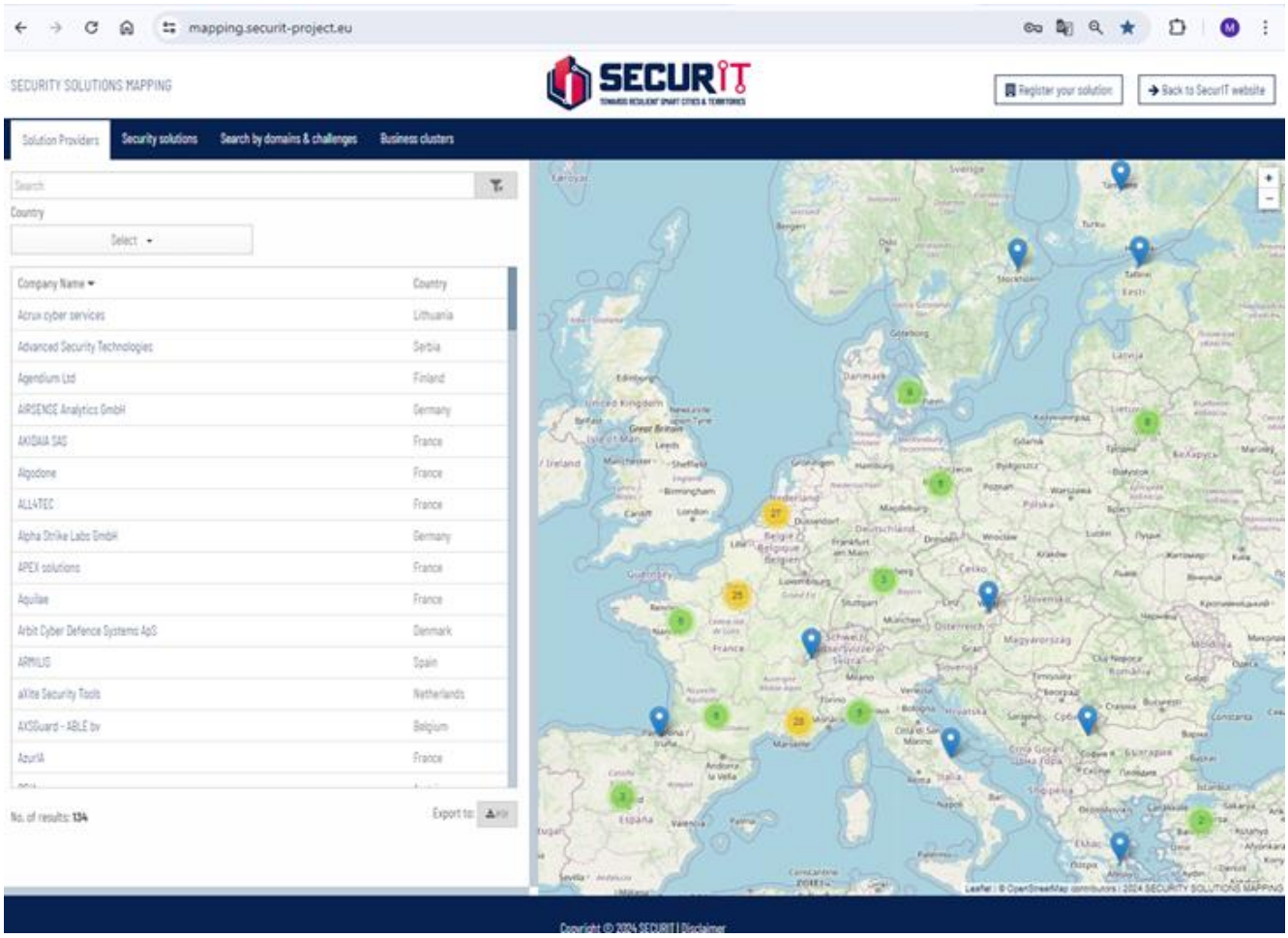
Other security products and solutions:

- Identification and authentication
- Intruder detection and alarm/Fire detection
- Detection and screening for dangerous or illicit items or concealed persons
- Observation and surveillance (localised)
- Observation and surveillance (wide area)
- Tracking and, tracing, positioning and localisation
- Tracking, localisation and positioning of hazardous substances and devices
- Command, control and decision support
- Intelligence and information gathering
- Vehicles and platforms (e.g.: aircraft; UAVs; robotic platforms)
- Equipment and supplies for security services

The solutions proposed have been captured by the consortium in the publicly available SecurIT mapping platform Securit-project.eu, designed to help users with needs and supply chain partners including SMEs with innovative solutions to connect and collaborate. The platform and mapping process is described in more detail, including the company and solution registration process, in deliverables *D2.3 Cybersecurity and security sector offers analysis 1 - Mapping of security solutions offers* and *D2.4 Cybersecurity and security sector offers analysis 2 - Mapping of security solutions offers)*. Figure 1 shows a platform view displaying SME solution providers and their locations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 1 - SecurIT mapping platform view example: SME solution providers and locations



https://mapping.securit-project.eu/

As of 14th June 2024, the online interactive mapping of SecurIT solutions comprises 166 different security products/services, provided by 134 different companies (SMEs) from 15 different countries:

- Austria
- Belgium
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Italy
- Lithuania
- Netherlands
- Poland
- Serbia
- Sweden
- Turkey

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

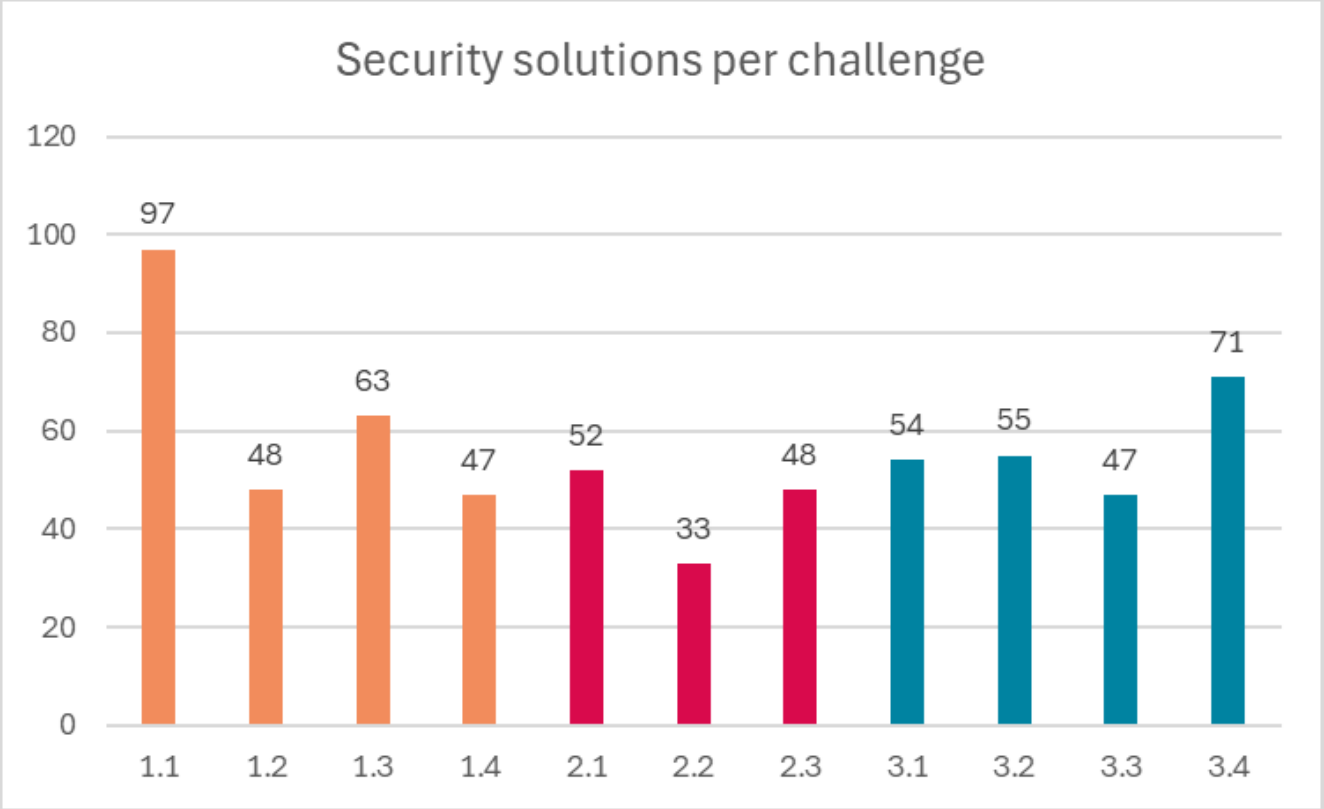
The 166 security products/services mapped and promoted on the SecurIT online platform (as of June 14th 2024) represents a high proportion of the solutions offered in 241 proposals into the Open Calls, and significantly exceeds the SecurIT target outcome of generating at least 50 innovative SME solutions to address user needs.

The distribution of these identified security solutions among the SecurIT Challenges is shown in Figure 2 and Figure 3 (*each solution can belong to several challenges*).

Figure 2 - SecurIT Challenges

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 3 – Security solutions per challenge

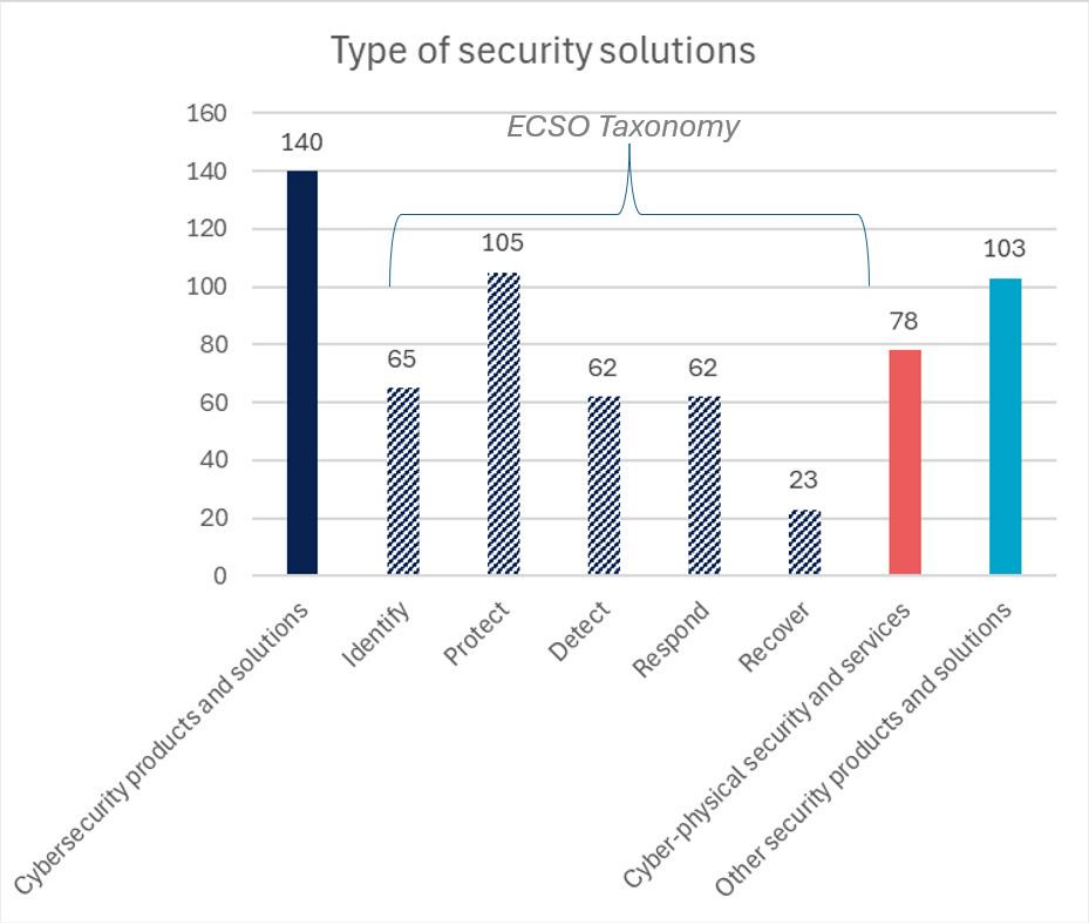


The 166 security products/services mapped and promoted on the SecurIT online platform address all of the challenges identified by SecurIT. The highest number of solutions (97) addresses Cybersecurity for Sensitive Infrastructure Protection (Challenge 1.1) while the lowest number of solutions is for Communication and Warning Systems during a crisis (Challenge 2.2).

These 166 security solutions have also been classified in terms of solution types (functions) to see if there are shortfalls in competency terms, as presented in Figure 4 (*each solution can belong to several solution types)*.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 4 – Numbers of SecurIT solutions mapped against technology competences.



The 166 security products/services mapped and promoted on the SecurIT online platform cover all of the solution types defined in the above taxonomy. The lowest number of solutions (23) address the recovery phase after a Cyber Physical attack.

2.4 Regional strengths and weaknesses

This section is dedicated to the findings from work in the Task 2.3. The Task was dedicated to an analysis of European Structural and Investment Funds (ESIF) and aligned them with a portfolio of funded SMEs. During the Task implementation and overall implementation of the project some relevant challenges and gaps were identified. Detailed results are presented in the project deliverable *D2.5 Synergy analysis with ESIF*. During the Task implementation and overall implementation of the project some relevant challenges and gaps were identified.

Initial work included mapping projects to two types of documents: funding instrument documents and strategic documents. It was thought that strategic documents could provide valuable insights into market potential driven by their unique security concerns and threat landscapes. The link with funding instruments was more obvious. In most cases funding instruments were described in two different levels – programs and calls. Programs provide the more abstract definitions of the funding intentions, while calls can be mapped to the interests of the SME's. Mapping activities and analysis carried out provided some conclusions.

- From the perspective of the SME strategic documents and program level descriptions of funding instruments are of a limited relevance to SME's. Both are too complex and are not providing relevant condensed information for solution providers.
- The other finding is about the primary intent – to identify some regional differences that could provide some insights for SME's in their development. Any significant indications on differences were not identifiable on the level of strategic documents. Priorities in security related sectors are very similar, and technologies supported

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

also very similar. There are some differences at funding level, but they do not provide any reasonable insights for the regional strengths.

Another subject for analysis was SecurIT project ecosystem, clusters (8 clusters) and their services in particular. This analysis indicated that at this point of time the clusters are focused on rather traditional services: networking, access to funding, hosting of different events etc. All those are relevant for SME's, but no new, innovative services uniquely tailored to SMEs specific needs were identified during the analysis. Also, no significant differences across different MS's were observed.

Task 2.3 also analysed the success of SME support measures and identified barriers and challenges that SME's face developing offerings in the security sector, described in detail in D2.5. **The main SME barriers and challenges identified were:**

- **Difficulties in keeping pace with the complex and changing regulatory environment.**
- **Lack of understanding of end-user needs, requirements, and priorities by SMEs.**
- **Challenges maintaining and establishing new collaborations with relevant stakeholders.**
- **Very long innovation adoption times by end user organization that are longer than anticipated sales cycles.**
- **Financial restraints and limited access to financial instruments.**

In addition to general observations provided above, the main focus of Task 2.3 was to map funded projects against funding instruments at different levels. The methodology is provided in D2.5, but key insights gained during and after the implementation of the task are presented below:

- The Security sector can be characterised as having limited demand if we consider only the national or regional level. To grow, understand expectations of end-users and generate revenue needed for productization, SME's should go beyond the national boundaries. This is particularly relevant for smaller MS. Those activities require funding.
- SME's can access funding on the national or EU (or even wider, like NATO DIANA program) level. National funding instruments are mainly focused on the national level developments (or even regional in some cases), not supporting cross-border cooperation or joint initiatives. International level funding instruments are difficult to access, require extensive consortia, and require significant project management and application development skills and resources.
- Descriptions of funding instruments at EU and National levels are difficult to navigate for the SME's. Despite how well some national funding instruments are defined and structured, following the life cycle of innovation development, they lack the capacity to facilitate international collaboration and joint developments and do not provide space for moderation activities.

Implementation of the SecurIT project and identified success stories as presented in D2.5 allows us to identify some of the success factors:

- Cross-border cooperation can facilitate a higher rate of successful innovation development, as synergies can be generated from integrating relatively narrow solutions from providers.
- Mentoring and clustering services (described in D2.5) for SME's seem to be of significant importance.

A project clustering approach that enables SMEs to interact with end-users from various domains and MS obtaining instant feedback on the relevance of their solutions, while simultaneously presenting end-users with a wide array of innovative technologies tailored to their specific areas of interest, which they can select from, benefits both users and SME suppliers. Clusters of other eco-systems can provide SME's with important links with end-users and help with navigating different level funding instruments.

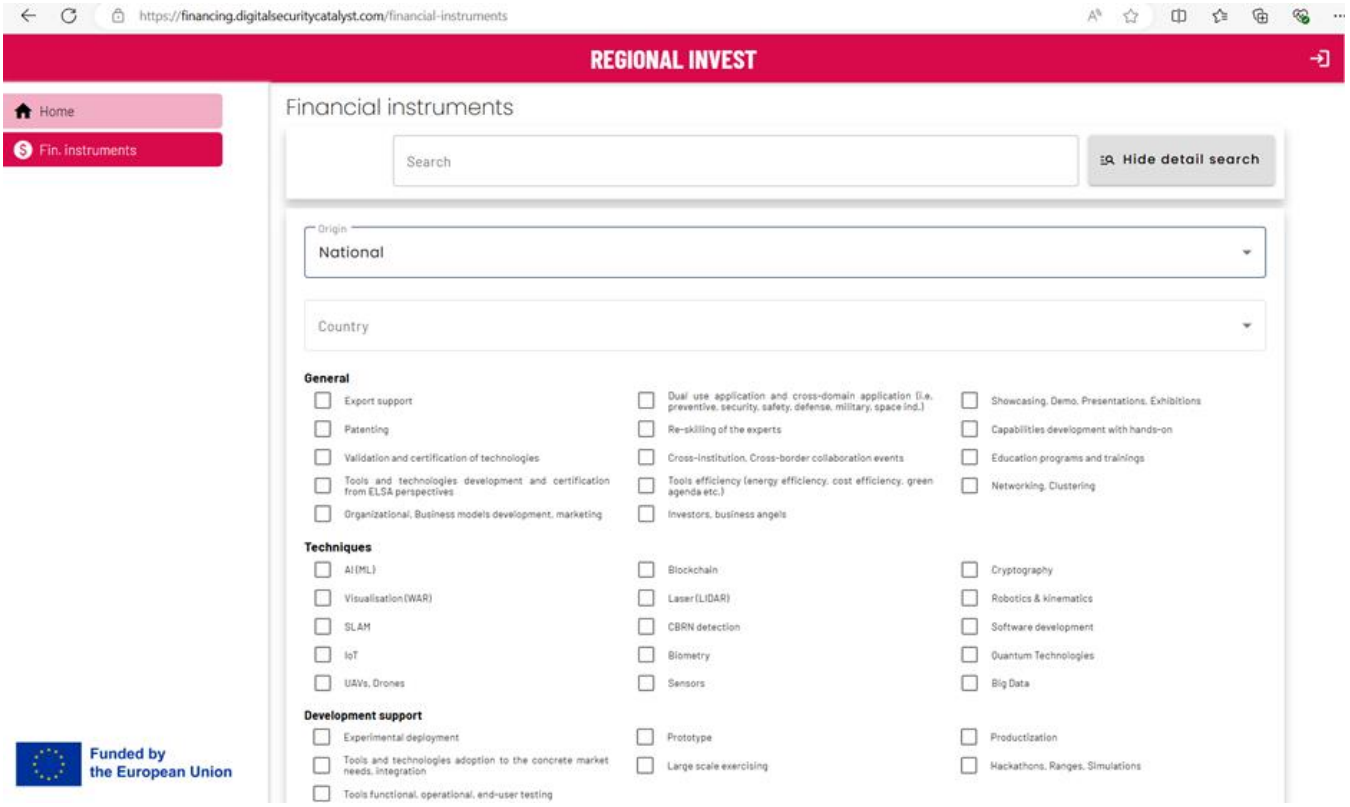
Going one step further, **use of different national funding instruments for joint development of innovations can also be very important factor of potential success.**

In Task 2.3 the idea of producing a tool to make it easier for SMEs to access different level funding instruments at regional, national and EU level was investigated, and a prototype tool was developed to implement this. One of the project partners – LSEC – volunteered to develop the tool working with a Belgian company "Co-dex". A simple tool was developed, **Regional Invest**, to allow initial selection by SME users of funding instruments and strategic documents of interest, and made available to all interested entities through the SecurIT web page (https://financing.digitalsecuritycatalyst.com). The entrance interface was designed to be very simple and functional

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

options contain only the searching and log-in possibilities. Figure 5 shows a view of the National Financial Instruments Search Page.

Figure 5 - Regional Invest SME Funding Tool View Example – National Funding Instrument search menu



It was felt that such a solution could ease the access to funding for SME's. At the same time it could facilitate cross-border cooperation and synergies from applying for national funding in such cross-border projects. To examine this discussions on the relevance of such a tool and its potential impact were held during the final stage of the project implementation. Presentations were made for different relevant organizations at national and EU levels. Those discussions proved the need for such a tool. At the same time, it was agreed that maintenance of such a solution appeared rather challenging.

SecurIT has identified the potential benefits of developing an online tool to make it easier for SMEs to access funding instruments at regional, national and EU level. Such a tool can help SMEs and SME consortia access cross-border funding sources and help SMEs to scale their security solutions. A prototype has been demonstrated to potential stakeholders, but a mechanism would need to be found to support the maintenance of such a system.

2.5 Open Call 1 and 2 Results

The following chapter identifies gaps based on the results of Open Call 1 and 2, more specifically the resulting applications received were subject to further analysis to learn from how the Open Call applications tried to respond to the earlier identified topics, and gaps and which remaining gaps still exist – but also which additional gaps have ben identified by these applicants.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

2.5.1 Open Call Process and Refinement

As described in Section 2.2 the SecurIT project used workshops in November 2021 and November 2022 involving integrators and end-users to define common gaps in cyber-physical security to be addressed by SMEs in two Open Calls for proposals issued in January 2022 and January 2022. Three application domains were defined, segmented into eleven specified sub-domains with clear challenges and areas of need as shown below, together with an 'other' category for other challenges not captured in SecurIT domains that SMEs identified as important and submitted proposals to address [1] [2]:

After Open Call 1, the SecurIT consortium analysed the Call results and the first selection process, aided by the Advisory Board, stakeholder input at the Open Call 2 workshop and SME bidder feedback, and as a result revised the Open Call challenges and refined the application process to make the user needs and guidance clearer and submission easier for SMEs [3]. The results are shown below.

2.5.2 Open Call Results – Addressing the User Challenges

2.5.2.1 Open Call 1 Results

Table 1 presents the bid results for Open Call 1 mapped against the security challenge domains that bidders sought to address, also shown in

[1] SecurIT Deliverable D2.1 - SecurIT challenges definition linked to Open call 1; December 2021
[2] SecurIT Deliverable D2,2 - D2.1 SecurIT challenges definition linked to Open call 2; December 2022
[3] SecurIT Deliverable D2,2 - D2.1 SecurIT challenges definition linked to Open call 1; December 2022

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

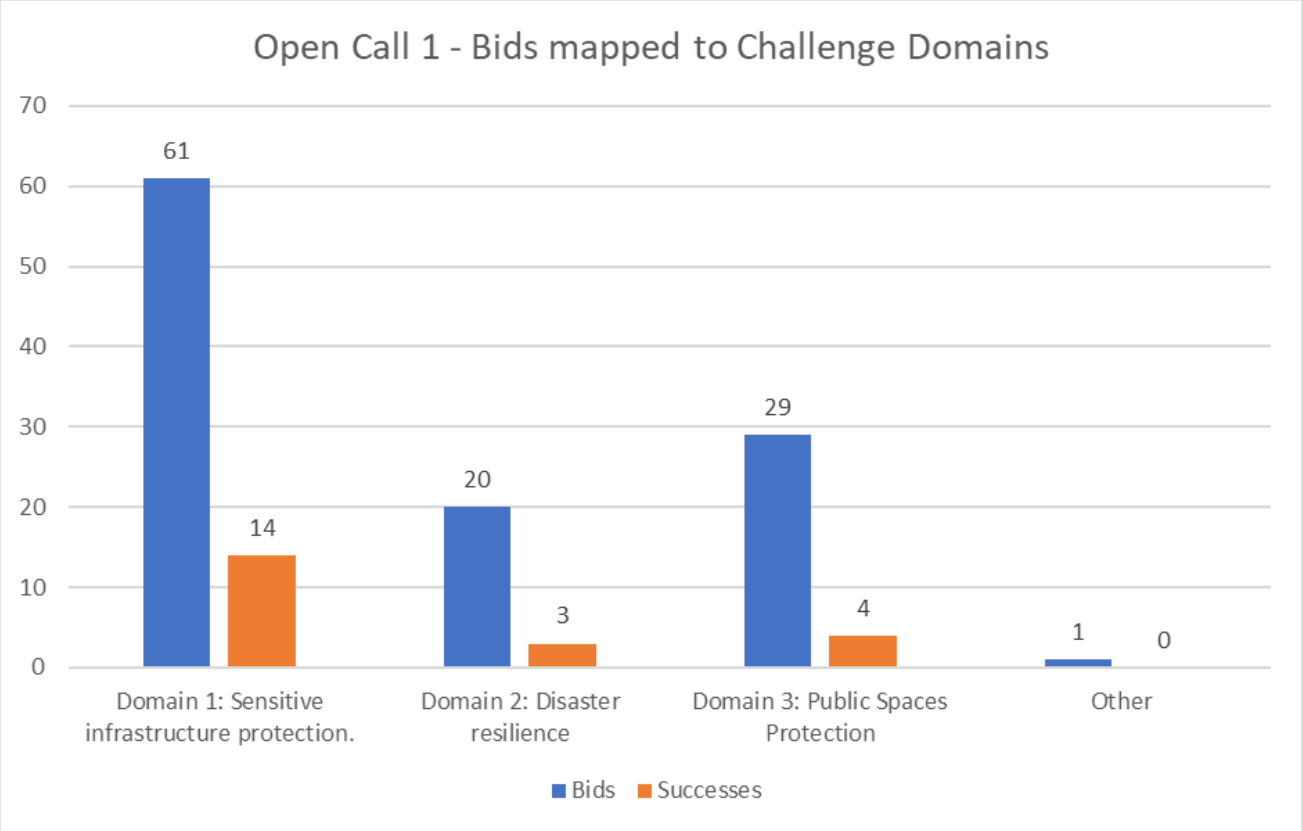
Figure 6.

Table 1 - Open Call 1 Bid Results mapped against Security Challenge domains.

Challenge Domain	Bids	Successes	Success Rate
Domain 1: Sensitive infrastructure protection.	61	14	23%
Domain 2: Disaster resilience	20	3	15%
Domain 3: Public Spaces Protection	29	4	14%
Other	1	0	0%
TOTAL	**111**	**21**	19%

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 6 - Open Call 1 Bid Results mapped against Security Challenge domains.



A total of 111 proposals were submitted into Open Call 1 and 21 were funded, a success rate of 19%. Sixty-one of the 111 proposals (55%) into Open Call 1 addressed Domain 1, Secure Infrastructure Protection, with significantly fewer bids (18% and 20% of bids respectively) into Disaster resilience (Domain 2) and Public Spaces Protection - Major Events (Domain 3). SME bidders were more comfortable bidding into the Secure Infrastructure Protection domain than Disaster resilience or Public Spaces Protection, either because they were more familiar with the secure infrastructure domain or their capabilities were more suited to it. The quality of proposals into the Secure Infrastructure Protection domain was also higher, with a 23% success rate compared to success rates of 15% for and 14% for Disaster resilience and Public Spaces Protection.

Table 2 presents the bid results for Call 1 mapped against the primary (core) security challenges that bidders sought to address, also shown in Figure 7.

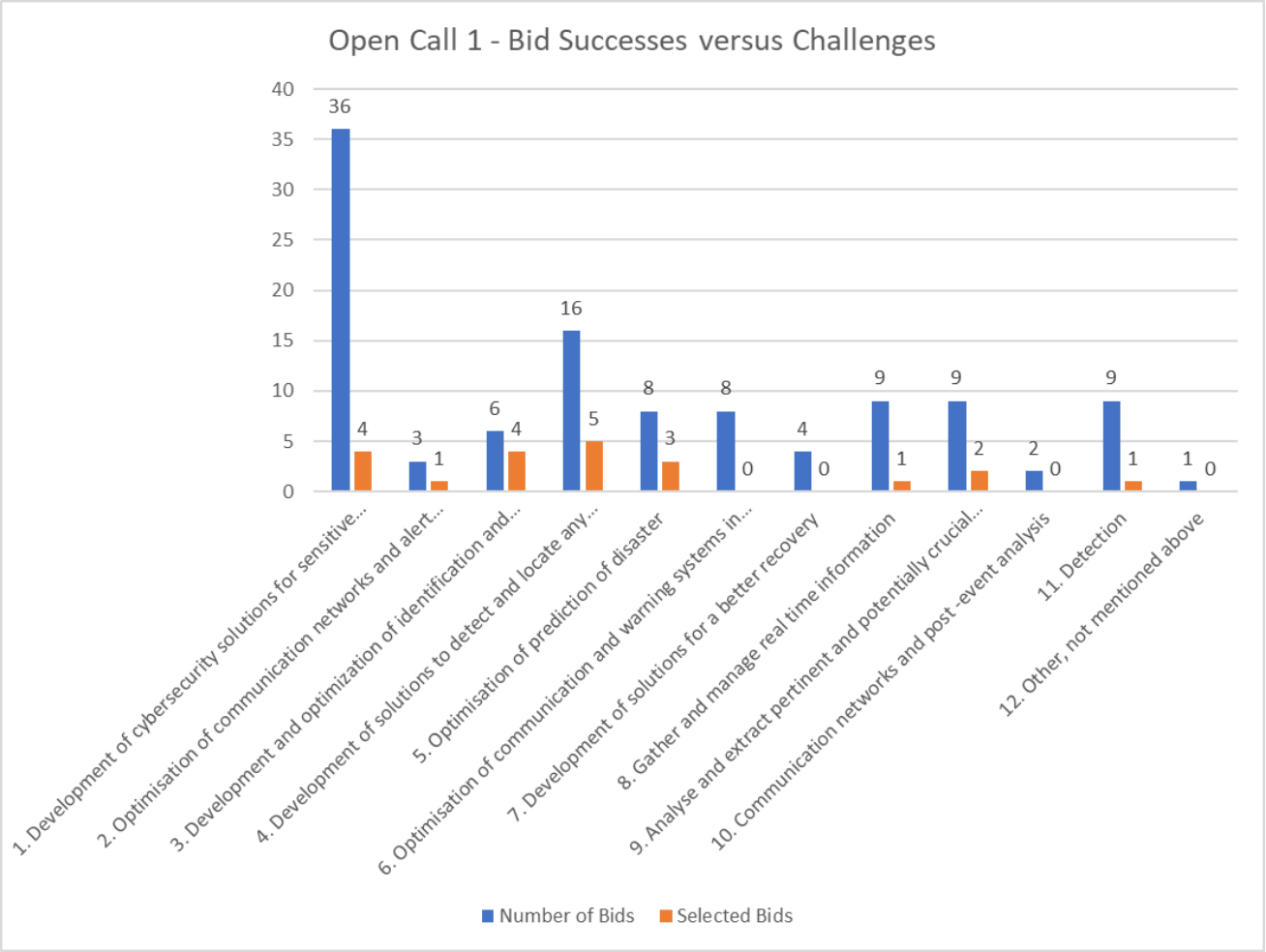
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table 2 – Open Call 1 Bid Results mapped against Primary (Core) Security Challenges

Challenge Domain	Primary (Core) Challenges addressed by proposals	Number of Bids	Selected Bids
Domain 1: Sensitive infrastructure protection	1. Development of cybersecurity solutions for sensitive infrastructure protection	36	4
	2. Optimisation of communication networks and alert systems	3	1
	3. Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk.	6	4
	4. Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions	16	5
Domain 2: Disaster resilience	5. Optimisation of prediction of disaster	8	3
	6. Optimisation of communication and warning systems in case of disaster	8	0
	7. Development of solutions for a better recovery	4	0
Domain 3: Public Spaces Protection - Major Events.	8. Gather and manage real time information	9	1
	9. Analyse and extract pertinent and potentially crucial information as quickly as possible	9	2
	10. Communication networks and post -event analysis	2	0
	11. Detection	9	1
Other	12. Other, not mentioned above	1	0
	TOTAL	**111**	**21 (19%)**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 7 - Open Call 1 Bid Results mapped against Primary (Core) Security Challenges.



In line with the lower number of SME bids into Disaster resilience and Public Spaces Protection - Major Events there were three gaps in the Open Call 1 funded portfolio of SME solutions, with no successful bids addressing three of the eleven challenges covering communications and disaster recovery as the main focus of their solution (core challenges):

6. Optimisation of communication and warning systems in case of disaster
7. Development of solutions for a better recovery
10. Communication networks and post-event analysis

After Open Call 1 the application process and guidance was revised to make submission easier for SMEs and to try to address gaps in portfolio coverage. The outcome is described below.

2.5.2.2 Open Call 2 Results

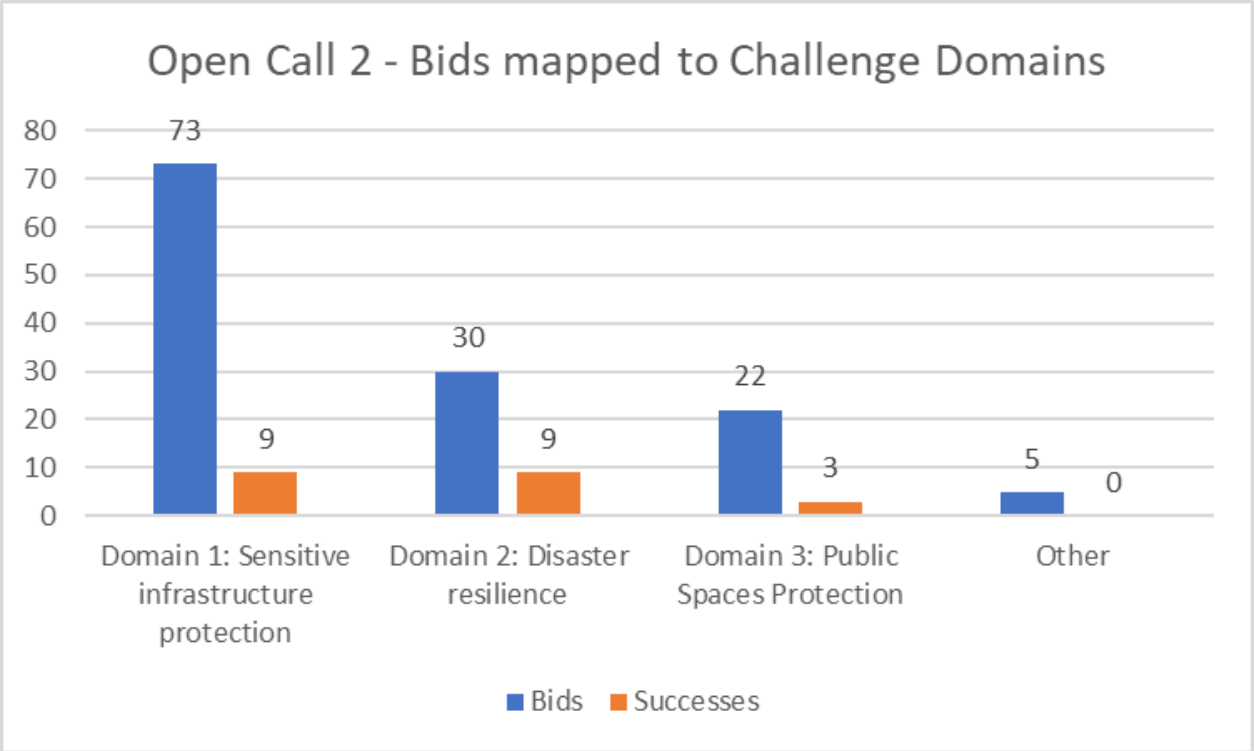
Table 3 presents the bid results for Open Call 2 mapped against the security challenge domains that bidders sought to address, also shown in Figure 8.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table 3 – Open Call 2 Bid Results mapped against Security Challenge domains.

Challenge Domain	Bids	Successes	Success Rate (%)
Domain 1: Sensitive infrastructure protection	73	9	12%
Domain 2: Disaster resilience	30	9	30%
Domain 3: Public Spaces Protection	22	3	14%
Other	5	0	0%
TOTAL	**130**	**21**	**16%**

Figure 8 – Open Call 2 Bid Results mapped against Security Challenge domains.



A total of 130 proposals were submitted into Open Call 2, a significantly higher level of interest than for Call 1, and 21 were funded, a success rate of 16%. Once again SME bidders focused on Domain 1, Secure Infrastructure Protection (56% of bids), with significantly fewer bids (23% and 17% of bids respectively) into Disaster resilience (Domain 2) and Public Spaces Protection - Major Events (Domain 3). However while the bid success rate for Public Spaces Protection was unchanged from Open Call 1, the bid success rate into Disaster resilience significantly increased to 30% (from 15%) in Open Call 2.

Table 4 presents the bid results for Call 2 mapped against the primary (core) security challenges that bidders sought

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

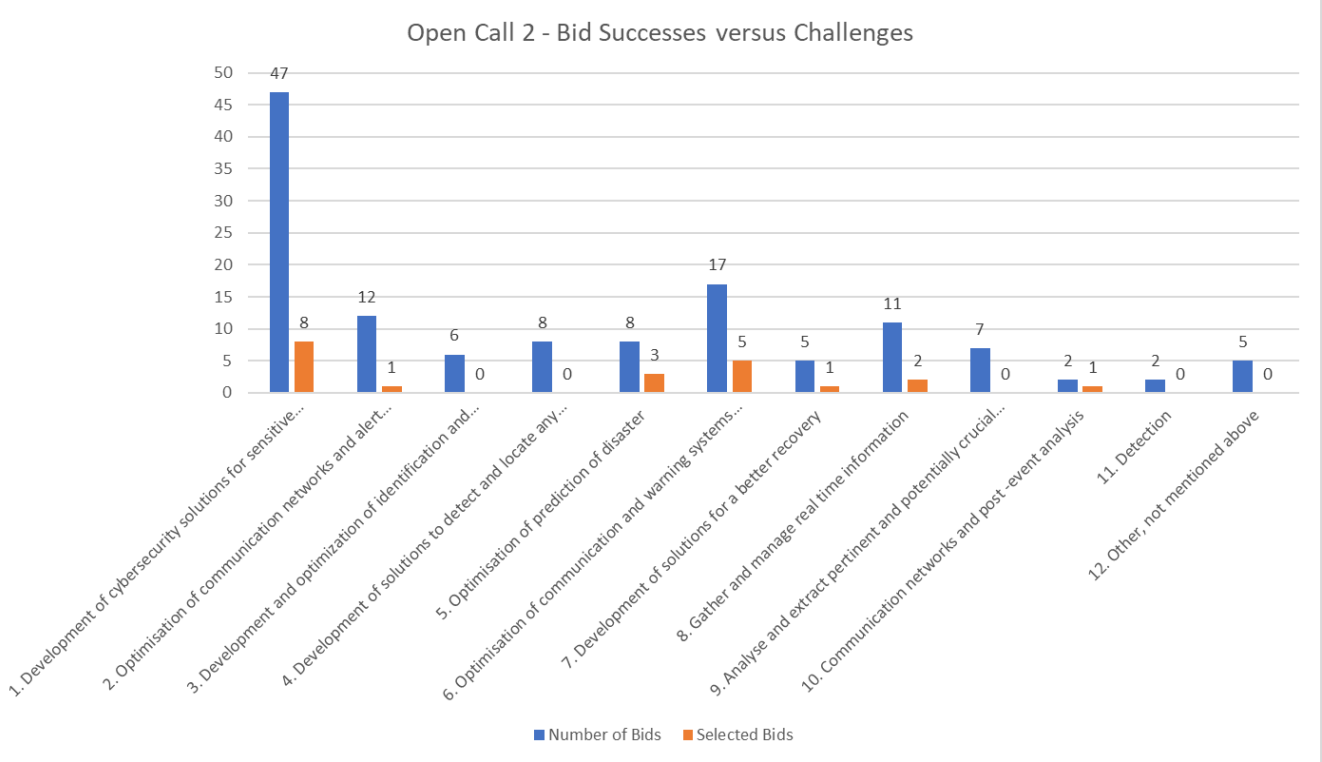
to address, also displayed in Figure 9.

Table 4 – Open Call 2 Bid Results mapped against Primary (Core) Security Challenges.

Challenge Domain	Primary (Core) Challenges addressed by proposals	Number of Bids	Selected Bids
Domain 1: Sensitive infrastructure protection	1. Development of cybersecurity solutions for sensitive infrastructure protection	47	8
	2. Optimisation of communication networks and alert systems	12	1
	3. Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk	6	0
	4. Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions	8	0
Domain 2: Disaster resilience	5. Optimisation of prediction of disaster	8	3
	6. Optimisation of communication and warning systems in case of disaster	17	5
	7. Development of solutions for a better recovery	5	1
Domain 3: Public Spaces Protection - Major Events.	8. Gather and manage real time information	11	2
	9. Analyse and extract pertinent and potentially crucial information as quickly as possible	7	0
	10. Communication networks and post -event analysis	2	1
	11. Detection	2	0
Other	12. Other, not mentioned above	5	0
	TOTAL	**130**	**21 (16%)**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 9 – Open Call 2 Bid Results mapped against Primary (Core) Security Challenges.



Four of the security challenges posed by users had no successful solutions put forward in Call 2:

> 3. Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk
>
> 4. Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions
>
> 9. Analyse and extract pertinent and potentially crucial information as quickly as possible
>
> 11. Detection

2.5.2.3 Combined Open Call 1 and 2 Results and Gap Analysis

This section looks at the combined results of Open Calls 1 and 2 to assess how well the solutions offered by SMEs addressed the user challenges identified by SecurIT and draws conclusions on capability gaps.

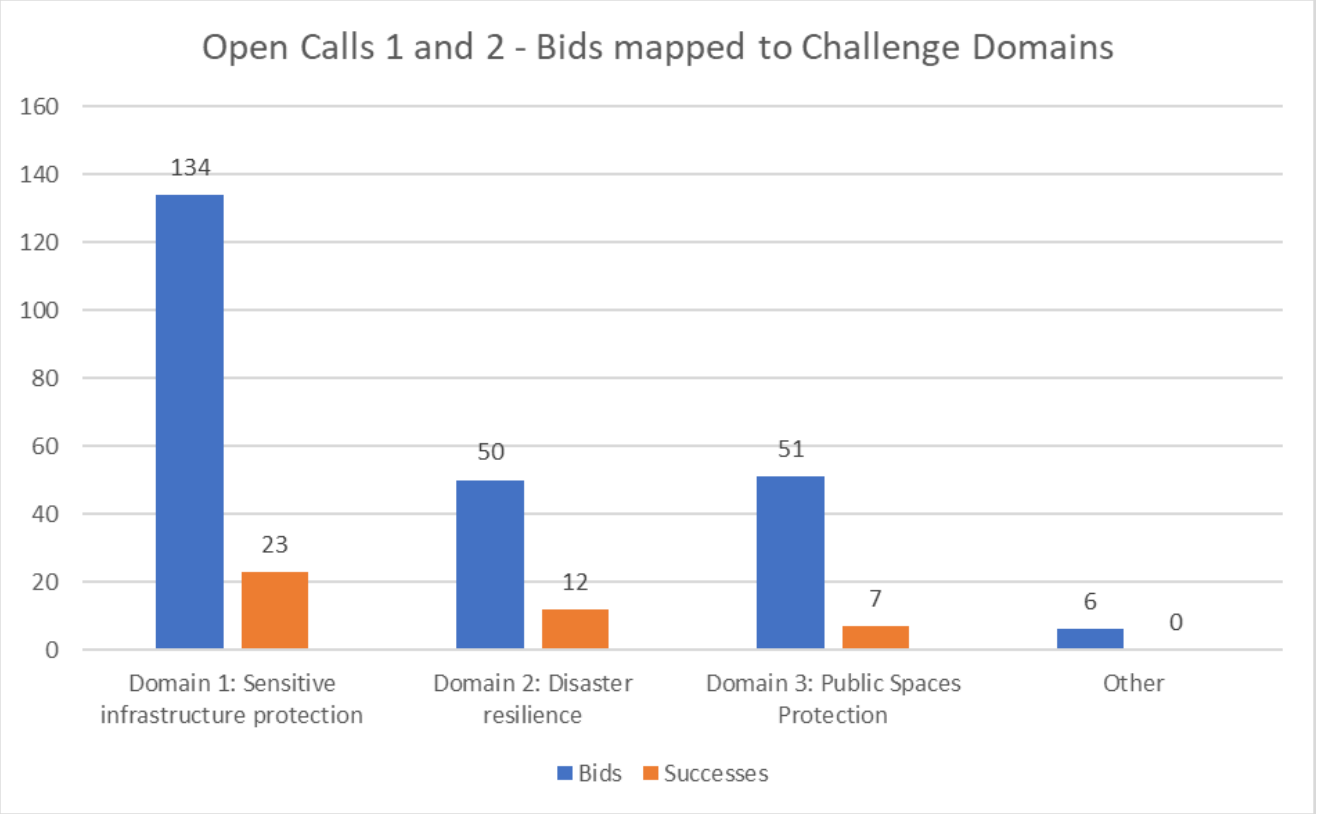
Table 5 presents the bid results for Open Calls 1 and 2 mapped against the security challenge domains that bidders sought to address, also shown in Figure 10.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table 5 - Open Call 1 and 2 Bid Results mapped against Security Challenge domains.

Challenge Domain	Bids	Successes	Success Rate
Domain 1: Sensitive infrastructure protection.	134	23	17%
Domain 2: Disaster resilience	50	12	24%
Domain 3: Public Spaces Protection	51	7	14%
Other	6	0	0%
TOTAL	**241**	**42**	**17%**

Figure 10 - Open Call 1 and 2 Bid Results mapped against Security Challenge domains.



A total of 241 proposals were submitted into Open Calls 1 and 2 and 42 were funded, a success rate of 17%. **For both Open Calls SME bidders were more comfortable bidding into the Secure Infrastructure Protection domain (55% of bids) than Disaster resilience (21% of bids) or Public Spaces Protection (21% of bids), either because they were more familiar with the secure infrastructure domain or their capabilities were more suited to it.**

Table 6 describes the Open Call 1 and 2 Bid Results mapped against Primary (Core) Security Challenges, as shown in Figure 11.

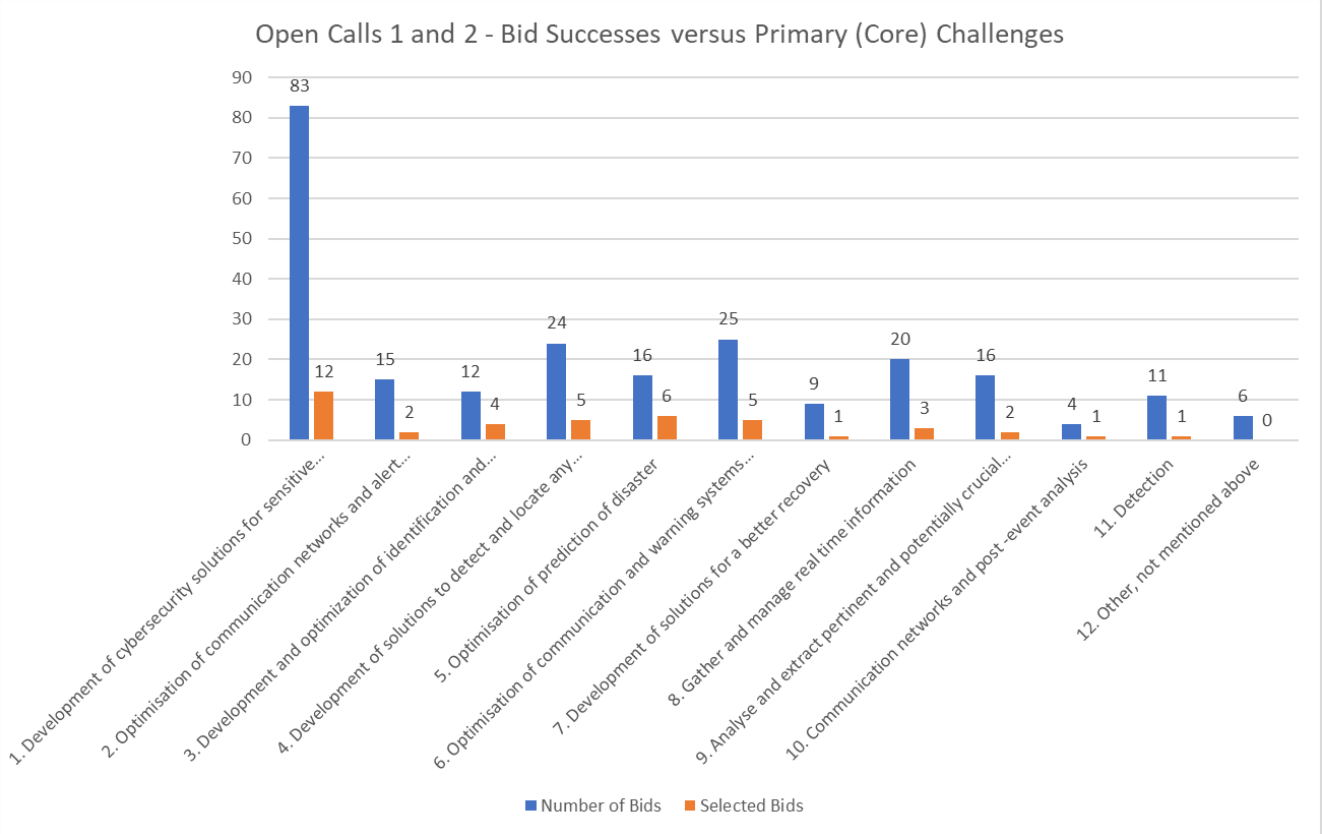
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table 6 - Open Call 1 and 2 Bid Results mapped against Primary (Core) Security Challenges.

Challenge Domain	Primary (Core) Challenges addressed by proposals	Number of Bids	Selected Bids	Success Rate (%)
Domain 1: Sensitive infrastructure protection	1. Development of cybersecurity solutions for sensitive infrastructure protection	83	12	14%
	2. Optimisation of communication networks and alert systems	15	2	13%
	3. Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk	12	4	33%
	4. Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions	24	5	21%
Domain 2: Disaster resilience	5. Optimisation of prediction of disaster	16	6	38%
	6. Optimisation of communication and warning systems in case of disaster	25	5	20%
	7. Development of solutions for a better recovery	9	1	11%
Domain 3: Public Spaces Protection - Major Events.	8. Gather and manage real time information	20	3	15%
	9. Analyse and extract pertinent and potentially crucial information as quickly as possible	16	2	13%
	10. Communication networks and post -event analysis	4	1	25%
	11. Detection	11	1	9%
Other	12. Other, not mentioned above	6	0	0%
	TOTAL	**241**	**42**	**17%**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 11 - Open Call 1 and 2 Bid Results mapped against Primary (Core) Security Challenges.



Key points are:

- Development of cybersecurity solutions for Infrastructure Protection (Challenge 1) dominated bidding (35% of bids).
- Communications networks and post-event analysis for Public Space Protection (Challenge 10) was not a popular bid topic (1.5% of bids).
- Open Call 2 was successful in attracting enough proposals into the Open Call 1 solution gaps (Challenges 6, 7 and 10) to be able to fund solutions tackling these challenges.

All three challenge gaps in the Open Call 1 funded portfolio of SME solutions were filled by solutions funded by Open Call 2. All eleven user security challenges being addressed by SecurIT have been met by at least one solution in Open Call 1 or Open Call 2 that addressed that challenge as its primary (core) challenge and was funded.

In addition, for most bids bidders stated that their solution, while aimed at one core challenge, was also relevant to other secondary challenges, with some cases of bids being relevant to five or more challenges. See Table 7 and Figure 12.

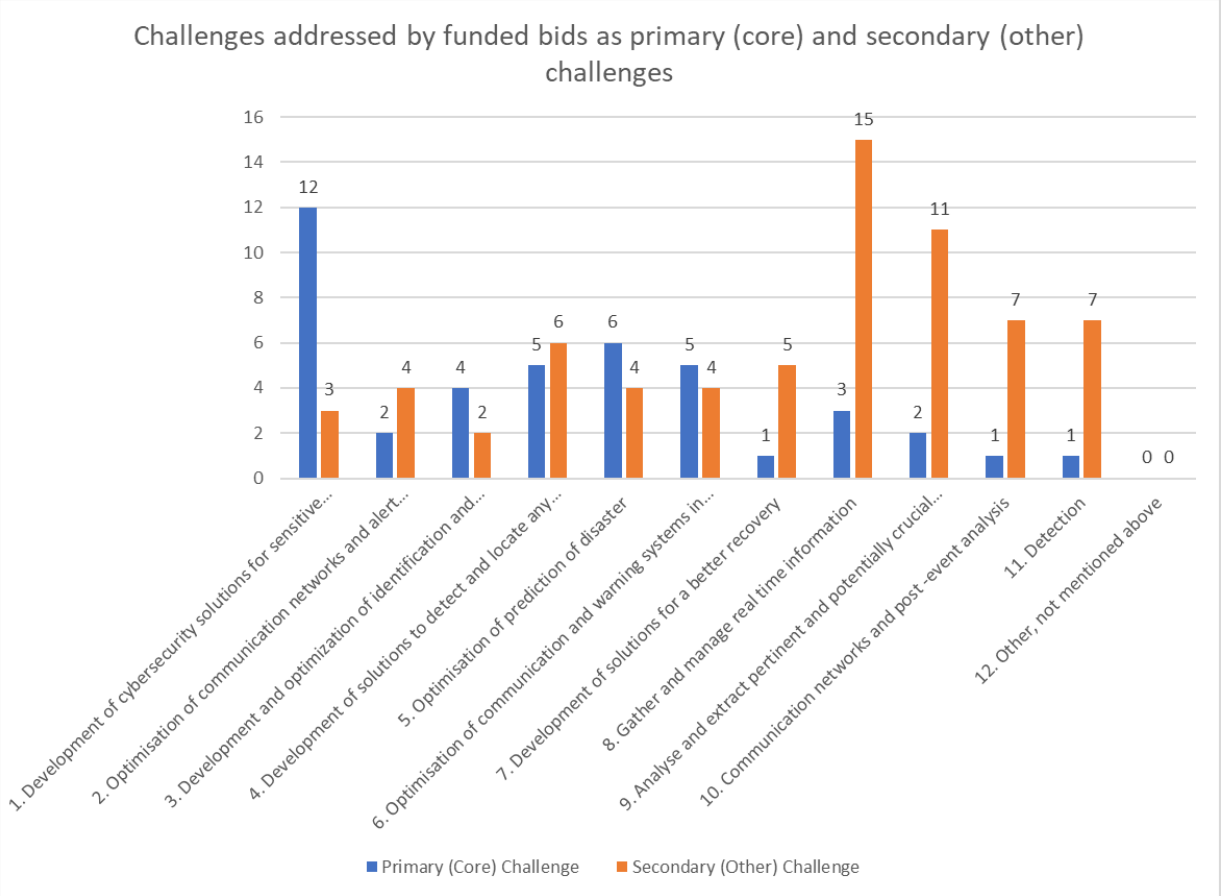
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table 7 – Funded bids mapped against core and secondary challenges.

Challenges addressed by funded bids	Primary (Core) Challenge	Secondary (Other) Challenge	Total of funded bids addressing Challenge
1. Development of cybersecurity solutions for sensitive infrastructure protection	12	3	15
2. Optimisation of communication networks and alert systems	2	4	6
3. Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk.	4	2	6
4. Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions	5	6	11
5. Optimisation of prediction of disaster	6	4	10
6. Optimisation of communication and warning systems in case of disaster	5	4	9
7. Development of solutions for a better recovery	1	5	6
8. Gather and manage real time information	3	15	18
9. Analyse and extract pertinent and potentially crucial information as quickly as possible	2	11	13
10. Communication networks and post -event analysis	1	7	8
11. Detection	1	7	8
12. Other, not mentioned above	0	0	0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 12 - Funded bids mapped against core and secondary challenges.

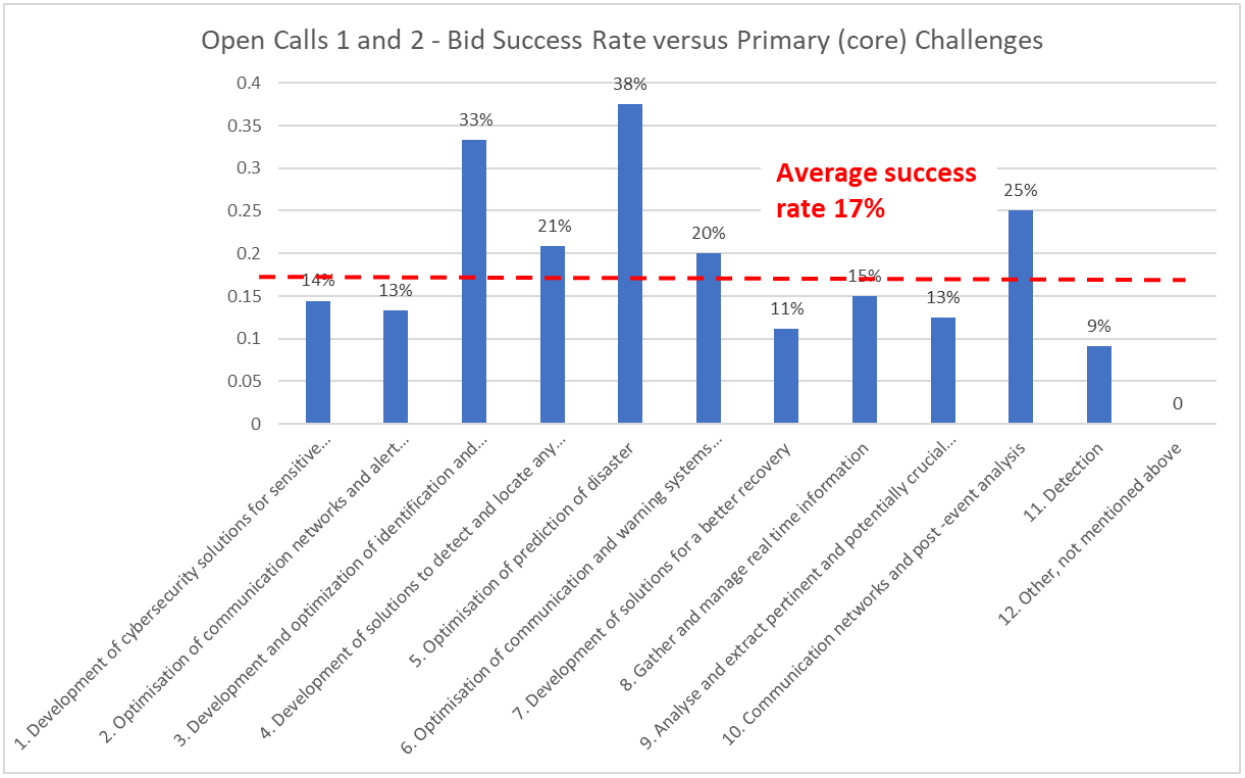


If one takes secondary (other) challenges into account the funded SecurIT portfolio of bids addresses all of the challenges with at least six solutions, either as core or secondary applications of the funded solutions.

If one looks at the relative quality of bids into the user challenges presented by SecurIT to SMEs, measured by bid success rates as described in Table 6, the results are shown in Figure 13.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 13 – Open Calls 1 and 2 – Bid Success Rate versus primary challenges.



Bid success rates for the development and optimization of identification and access control for rapid access in the [Secure Infrastructure] site etc (Challenge 3) and Optimisation of prediction of disaster (Challenge 5) were much higher (33% and 38%) than the call average (17%), while the bid success rate (9%) for Detection methods (data protection and cybersecurity/cybercrime) for public space major event protection (Challenge 11) was much lower. However the numbers of bids were not sufficient for these bid success variations to be determined to be statistically significant.

2.5.3 Open Call Results – Solution Technologies

2.5.3.1 Methodology

The technologies used in the SecurIT Open Calls have been analysed using an ENISA technology taxonomy that was developed in 2021 to support the definition of a taxonomy for ICT products to be used in the EUCC scheme. These technologies were defined by ENISA[4] as being particularly challenging for the security of ICT products and

[4] ENISA, GUIDANCE REPORT ON A TAXONOMY FOR ICT PRODUCTS APPLICABLE TO THE EUCC SCHEME, March 2021.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

systems (including areas where future developments can bring new security challenges) and are as follows:

1. Artificial intelligence and Machine Learning systems;
2. Radio technologies (e.g. 5G Networks , Short dedicated range communications);
3. Cloud, Edge and Virtualization;
4. Industrial Systems (e.g. IACS, OT, etc.);
5. Internet of Things;
6. Vehicular Systems (e.g. autonomous vehicles);
7. Database technologies, Business Intelligence and Big Data;
8. Blockchain and Distributed Ledger Technology (DLT);
9. Nanotechnology;
10. Satellite systems and applications;
11. Robotics;
12. Quantum Technologies (e.g. computing and communication);
13. Cybersecurity (e.g. Detection, Biometrics);
14. Other general technologies.

This taxonomy was tested for Open Call 1 and proved effective for studying the technology content of solutions bid into the SecurIT programme. As there were a significant number of additional common technologies used in the Call 1 bids the 'Other general technologies' technology component was broken down into sub-components to provide an enhanced technology description of the SecurIT bids, as follows:

14) - Modelling and Simulation (e.g. Digital Twins, VR/Metaverse);

15) - Situational Awareness (for decision support, C2 etc), Surveillance and Sensors

16) - Command and Control (of teams, people e.g. Crisis Management)

17) - Other

2.5.3.2 Combined Open Call 1 and 2 Results

The technologies used in the 241 Open Call 1 and 2 bids are described in Table 8 and shown in Figure 14, ranked in order of the frequency of their use.

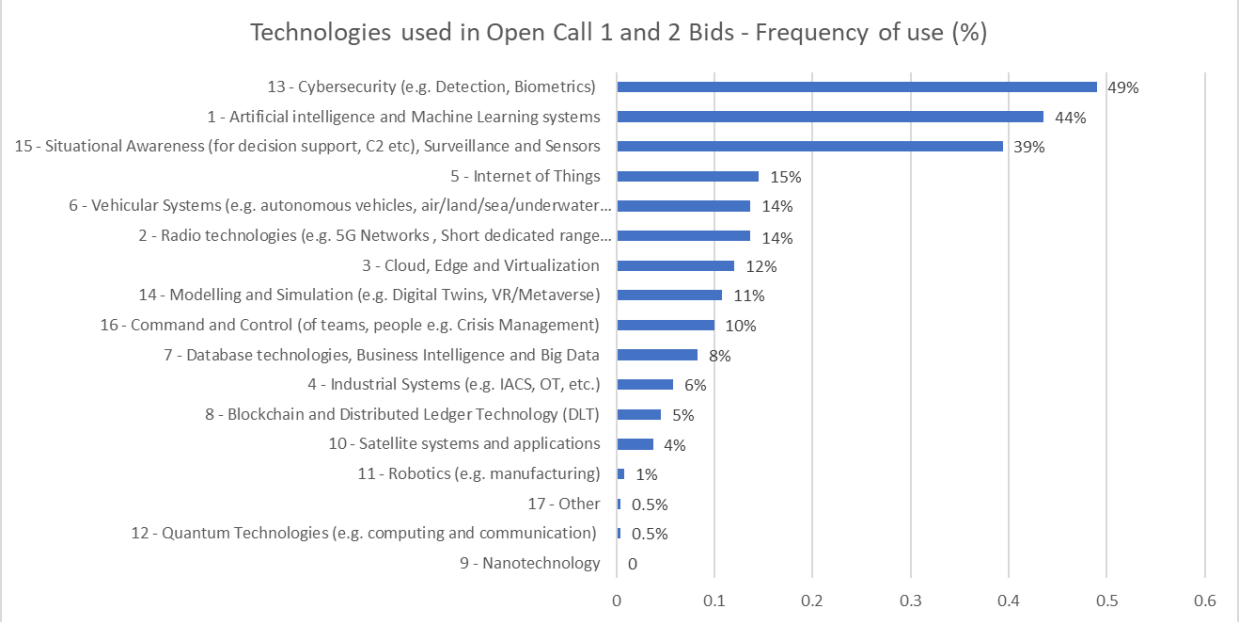
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table 8 – Solution technologies used in SecurIT bids – bid numbers and bid frequency.

Technology	Bid Percentage	Bid Number
13 - Cybersecurity (e.g. Detection, Biometrics)	49%	118
1 - Artificial intelligence and Machine Learning systems	44%	105
15 - Situational Awareness (for decision support, C2 etc), Surveillance and Sensors	39%	95
5 - Internet of Things	15%	35
2 - Radio technologies (e.g. 5G Networks , Short dedicated range communications)	14%	33
6 - Vehicular Systems (e.g. autonomous vehicles, air/land/sea/underwater drones, balloons, traffic management of vehicles)	14%	33
3 - Cloud, Edge and Virtualization	12%	29
14 - Modelling and Simulation (e.g. Digital Twins, VR/Metaverse)	11%	26
16 - Command and Control (of teams, people e.g. Crisis Management)	10%	24
7 - Database technologies, Business Intelligence and Big Data	8%	20
4 - Industrial Systems (e.g. IACS, OT, etc.)	6%	14
8 - Blockchain and Distributed Ledger Technology (DLT)	5%	11
10 - Satellite systems and applications	4%	9
11 - Robotics (e.g. manufacturing)	1%	2
12 - Quantum Technologies (e.g. computing and communication)	0.5%	1
17 - Other	0.5%	1
9 - Nanotechnology	0%	0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Figure 14 – Solution technologies used in SecurIT bids – bid numbers and bid frequency.



Key points are:

- Cybersecurity (detection, biometrics etc) technologies (49% of bids), Artificial Intelligence and Machine Learning system technologies (44%) and Situational Awareness, Surveillance and Sensors technologies (39%) were those most frequently offered to address the SecurIT challenges.
- There was significant use by SMEs of Cloud, Edge and Virtualization technologies (12% of bids), Modelling and Simulation technologies (11%), Command and Control technologies and Database (10%), and Business Intelligence and Big Data technologies (8%)
- There was little use of Robotic technologies (1% of bids) and Quantum Technologies (0.5% of bids) and no use of Nanotechnology in the SME bids.

It is possible to use a technology taxonomy approach to look at whether technologies are being used and exploited by SMEs to solve user challenges as shown above, but it is also possible to use this technique to study combinations of technologies used in bids. For example:

- SMEs offering Cybersecurity technologies in their solutions also made frequent use (43% of cases) of AI/ Machine Learning technologies. **AI/ Machine Learning was used extensively by SMEs when solving Cybersecurity challenges.**
- SMEs offering Physical Surveillance technologies in their solutions also made frequent use (47% of cases) of AI/ Machine Learning technologies. **AI/ Machine Learning was used extensively by SMEs when solving Physical Surveillance challenges.**
- Blockchain/ Distributed Ledger Technology was not used by SMEs in any of the solutions that used Command and Control technologies.

2.5.4 Open Call 1 and 2 analysis: Conclusions and potential Gaps between supply and demand

Key points are as follows:

1) Domain Responses. A total of 241 proposals were submitted into Open Calls 1 and 2 and 42 were funded, a success rate of 17%. **For both Open Calls SME bidders were more comfortable bidding into the Secure Infrastructure Protection domain (55% of bids) than Disaster resilience (21% of bids) or Public Spaces Protection (21% of bids), either because they were more familiar with the secure infrastructure domain or their capabilities were more suited to it.**

2) Challenge Responses. In Open Call 1, in line with the lower number of SME bids into Disaster resilience and Public Spaces Protection - Major Events there were **three gaps in the Open Call 1 funded portfolio of SME solutions**, with no successful bids addressing three of the eleven challenges covering communications and disaster recovery as the main focus of their solution (core challenges):

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

6. Disaster resilience - During the crisis: Mass communication and warning systems: Optimisation of communication and warning systems in case of disaster.

7. Disaster resilience - After the crisis: Post event analysis and recovery: Development of solutions for a better recovery.

10. Public Spaces Protection – Major Events - Command and control (resource management) and decision- making support: Communication networks and post-event analysis.

After Open Call 1 the application process and guidance was revised to make submission easier for SMEs and to try to address gaps in portfolio coverage. All three challenge gaps in the Open Call 1 funded portfolio of SME solutions were then filled by solutions funded by Open Call 2. **All eleven user security challenges being addressed by SecurIT have been met by at least one funded solution in Open Call 1 or Open Call 2 that addressed that challenge as its primary (core) challenge.**

In addition, for most bids bidders stated that their solution, while aimed at one core challenge, was also relevant to other secondary challenges, with some cases of bids being relevant to five or more challenges. **If one takes secondary (other) challenges into account the funded SecurIT portfolio of bids addresses all of the challenges with at least six solutions, either as core or secondary applications of the funded solutions.**

3) Technologies used by SMEs to address user challenges. The technologies used in the SecurIT Open Calls have been analysed using an ENISA technology taxonomy. Key points are:

- Cybersecurity (detection, biometrics etc) technologies (49% of bids), Artificial Intelligence and Machine Learning system technologies (44%) and Situational Awareness, Surveillance and Sensors technologies (39%) were those most frequently offered to address the SecurIT challenges.
- SMEs offering Cybersecurity technologies in their solutions also made frequent use (43% of cases) of AI/ Machine Learning technologies. AI/ Machine Learning was used extensively by SMEs when solving Cybersecurity challenges.
- SMEs offering Physical Surveillance technologies in their solutions also made frequent use (47% of cases) of AI/ Machine Learning technologies. AI/ Machine Learning was used extensively by SMEs when solving Physical Surveillance challenges.
- There was significant use by SMEs of Cloud, Edge and Virtualization technologies (12% of bids), Modelling and Simulation technologies (11%), Command and Control technologies and Database (10%), and Business Intelligence and Big Data technologies (8%).
- Blockchain/ Distributed Ledger Technology was not used by SMEs in any of the solutions that used Command and Control technologies, but was used in 5% of bids overall.
- There was little use of Robotics technology (1% of bids) in their own right but these technologies may have been incorporated as components within the Vehicular Systems bids (14% of bids) which included autonomous vehicles;
- There was little use of Quantum Technologies (0.5% of bids) and no explicit use of Nanotechnology in the SME bids.

2.6 Conclusions and potential Gaps identified by SecurIT

Key points are:

- SecurIT has published a **Repository of Security and Cybersecurity Requirements** that presents common gaps and needs identified by security practitioners for the **Sensitive Infrastructure Protection, Disaster Resilience and Public Space Protection (Major Events) domains** that offer opportunities for SME innovations and address security threats to citizens. Annex 2 presents the final version of the challenges as used in Open Call 2. See Section 2.2.
- The 166 security products/services mapped and promoted on the SecurIT online platform (as of June 14th 2024) represents a high proportion of the solutions offered in 241 proposals into the Open Calls, and **significantly exceeds the SecurIT target outcome of generating at least 50 innovative SME solutions to address user needs.** See Section 2.3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

- **The 166 security products/services mapped and promoted on the SecurIT online platform address all of the challenges identified by SecurIT** (Section 2.3) if one considers the core and secondary challenges they address. The highest number of solutions (97) addresses Cybersecurity for Sensitive Infrastructure Protection (Challenge 1.1) while the lowest number of solutions is for Communication and Warning Systems during a crisis (Challenge 2.2).
- A **project clustering approach** (Section 2.4) that enables SMEs to interact with end-users from various domains and MS obtaining instant feedback on the relevance of their solutions, while simultaneously presenting end-users with a wide array of innovative technologies tailored to their specific areas of interest, which they can select from, benefits both users and SME suppliers. Use of different national funding instruments for joint development of innovations can also be a very important factor of potential success.
- SecurIT has identified the potential benefits of developing an **online tool to make it easier for SMEs to access funding instruments at regional, national and EU level** (Section 2.4). Such a tool can help SMEs and SME consortia access cross-border funding sources and help SMEs to scale their security solutions. A prototype (Regional Invest) has been demonstrated to potential stakeholders, but a mechanism would need to be found to support the maintenance of such a system.
- For both Open Calls **SME bidders were more comfortable bidding into the Secure Infrastructure Protection domain (55% of bids) than Disaster resilience (21% of bids) or Public Spaces Protection (21% of bids)**, either because they were more familiar with the secure infrastructure domain or their capabilities were more suited to it. See Section 2.5.
- **All eleven user security challenges being addressed by SecurIT have been met by at least one funded solution in Open Call 1 or Open Call 2 that addressed that challenge as its primary (core) challenge** (Section 2.5). If one takes secondary (other) challenges into account the funded SecurIT portfolio of bids addresses all of the challenges with at least six solutions, either as core or secondary applications of the funded solutions.
- SMEs made substantial use of important technologies, in particular Cybersecurity technologies (detection, biometrics etc) technologies (49% of bids), Artificial Intelligence and Machine Learning system technologies (44%) and Situational Awareness, Surveillance and Sensors technologies (39%) to address the SecurIT challenges (Section 2.5). **AI/ Machine Learning was used extensively by SMEs when solving Cybersecurity and Physical Surveillance challenges.**

Potential gaps between supply and demand identified by SecurIT are as follows:

1) SME solution application gaps – Communications, Warning, and Post-Event Recovery.

There were three gaps in the Open Call 1 funded portfolio of SME solutions, with no successful bids addressing three of the eleven challenges covering communications and disaster recovery as the main focus of their solution (core challenges). See Section 2.5. This resulted in the application process and guidance being revised to make submission easier for SMEs and to try to address gaps in portfolio coverage and this enabled these challenge gaps to be filled by solutions funded by Open Call 2. The challenges SMEs found difficult to successfully respond to initially were:

- Disaster resilience - During the crisis: Mass communication and warning systems: Optimisation of communication and warning systems in case of disaster.
- Disaster resilience - After the crisis: Post event analysis and recovery: Development of solutions for a better recovery.
- Public Spaces Protection – Major Events - Command and control (resource management) and decision-making support: Communication networks and post-event analysis.

2) SME business case/ technology gap – Limited use of Quantum Technologies.

In contrast to extensive use by SMEs of Artificial Intelligence and Machine Learning system technologies (44% of bids) there was limited use of Quantum Technologies (0.5% of bids) and no explicit use of Nanotechnology in the SME bids. See Section 2.5. Nanotechnology has limited relevance to the challenges being described but quantum technologies are relevant for new security sensors and secure computing and communications concepts. The Open Call response indicates that SMEs did not feel that the business case for using such technologies was strong enough

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

in terms of investment etc.

3) Other SME innovation gaps – regulation, end user understanding, collaboration building, slow innovation adoption, finance.

The main SME barriers and challenges identified (Section 2.4) were:

- Regulation - Difficulties in keeping pace with the complex and changing regulatory environment.
- End user understanding - Lack of understanding of end-user needs, requirements, and priorities by SMEs.
- Collaboration building - Challenges maintaining and establishing new collaborations with relevant stakeholders.
- Slow innovation adoption - Very long innovation adoption times by end user organization that are longer than anticipated sales cycles.
- Finance - Financial restraints and limited access to financial instruments.

3. GAP ANALYSIS

The following chapter will identify, compile and analyse the gaps identified in the different processes and will present an identification of gaps (SecurIT work and supporting desk research), how SecurIT tried to reach some closure of gaps through the SecurIT Open Calls and validating the results (by all partners) by engaging with Industry including End Users that qualified the Needs in the first half of the project

3.1 SecurIT Gap Results

Some Results from the Gap Analysis (Section 2) from the SecurIT Open Calls: SMEs were able to successfully respond to all the SecurIT user challenges presented to them for the Open Calls. All eleven user security challenges being addressed by SecurIT have been met by at least one solution in Open Call 1 or Open Call 2 that addressed that challenge as its primary (core) challenge and was funded. **No gaps in SME offerings to address user challenges defined by SecurIT were identified in the Open Call process.**

3.2 External Inputs on Gaps

3.2.1 Cybersecurity Gap analysis

A Cybersecurity Threat Map was defined by the European Commission 'Cybersecurity cOmpeteNCe fOr Research anD InnovAtion' (CONCORDIA) CSA project [5] in December 2022 [6]. See Table 9.

[5] https://cordis.europa.eu/project/id/830927
[6] www.concordia-h2020.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table 9 – Cybersecurity Threats

Domain (D)	Threat Group (TG)	Threats (T)
Device/IoT (1)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (2)
	Intentional Physical Damage (3)	Device modification (1) Extraction of private information (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Misuse of assurance tools (4) Failures of business process (5) Code execution and injection (unsecure APIs) (6)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1)
Network (2)	Unintentional damage / loss of information or IT assets (1)	Erroneous use or administration of devices and systems (1)
	Interception and unauthorised acquisition (2)	Signalling traffic interception (1) Data session hijacking (2) Traffic eavesdropping (3) Traffic redirection (4)
	Nefarious activity/abuse (3)	Exploitation of software bugs (1) Manipulation of hardware and firmware (2) Malicious code/software/activity (3) Remote activities (execution) (4) Malicious code - Signalling amplification attacks (5)
	Organisational (failure malfunction) (4)	Failures of devices or systems (1) Supply chain (2) Software bug (3)
System (3)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Configuration poisoning (1) Business process poisoning (2)

The project also identified the following technology-stack recommendations shown in Table 10.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table 10 – Technology-stack Recommendations

Number	Recommendation
R1	Focus on persistent threats
R2	Find a good trade-off between security level and domains peculiarities
R3	Tailored security investments
R4	Protection from insider threats
R5	Consider the deployment environment untrusted
R6	Digital twins and possible safety impact
R7	Protect user against profiling
R8	Protect the AI models, engines, and data pipelines from manipulations
R9	Consider the networking peculiarities while designing system security
R10	Protect from wide-band network-based localized DDoS
R11	Protect edge computing nodes and services
R12	Adoption of serverless computing
R13	Protect against AI weaponized threats
R14	Protection against deepfake
R15	Conscious use of Social Networks
R16	Deep understanding of layered architecture security
R17	Sharing and multi-tenancy concerns
R18	Consider the Virtualization/Containment weakness
R19	Control misconfiguration issues and foster transparency
R20	Avoid shadow IT
R21	Monitoring of human errors
R22	Continuous awareness campaign and training
R23	Protect the CIA triad of data
R24	Protect from mobile and IoT malware
R25	Adopt security-aware development pipelines
R26	Consider the complexity of the deployment environment
R27	Consider the miniaturization of the services
R28	Protect CPS devices

Most of these recommendations represent guidance, and not gaps in capabilities, technologies etc that could be addressed by investment of some form. Key gaps requiring further investment are assessed by SecurIT to be:

- Digital twins and possible safety impact;
- Protect the AI models, engines, and data pipelines from manipulations;
- Protect against AI weaponized threats;
- Protection against deepfake.

3.2.2 Cyber-Physical Security Gap analysis

The Horizon Europe Civil Security and Society programme is funding three Coordination and Support Actions to create Knowledge Networks, whose objectives include studying Cyber-Physical Security needs and challenges, as follows:

- European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection (EU-CIP) [7]; 1 October 2022 to 30 September 2025.
- Disaster Resilience Knowledge Network promoting innovation, technology uptake and multi-stakeholder cooperation (DIREKTION) [8]; 1 October 2023 to 30 September 2026.
- European Network Against Crime and Terrorism (ENACT) [9]; 1 September 2023 to 31 August 2026.

[7] European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection; https://cordis.europa.eu/project/id/101073878
[8] Disaster Resilience Knowledge Network promoting innovation, technology uptake and multi-stakeholder cooperation; https://cordis.europa.eu/project/id/101121249
[9] European Network Against Crime and Terrorism; https://cordis.europa.eu/project/id/101121152

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

These projects are all funded under Topic HORIZON-CL3-2021-SSRI-01-02, Knowledge Networks for Security Research & Innovation, and align well with the domains addressed by SecurIT:

1. Sensitive infrastructure protection;
2. Disaster resilience;
3. Public spaces protection – major events.

Key points that have emerged so far from these projects and are publicly available are summarised in the sub-sections below.

3.2.2.1 European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection (EU-CIP)

The objective of the EU-CIP project is to establish a pan European knowledge network for Resilient Infrastructures to support policy development and improve the innovation capacity of Critical Infrastructure (CI) operators, authorities, and innovators. The project is conducting desk research and analysis aimed at identifying gaps in Critical Infrastructure Protection (CIP) capability and knowledge. Preliminary analysis has identified CIP capability gaps/ needs in the following areas [10]:

1. enhanced adaptability,
2. reduced response times,
3. increased transparency of CIP solutions,
4. improved detection capabilities based on advanced analytics,
5. improved risk assessment capabilities to address asymmetric and hybrid threats,
6. capabilities addressing cascading effects across interconnected infrastructures,
7. support for proactive identification of threats based on real-time functions,
8. automated situation awareness based on multi-sensor inputs,
9. risk prediction functionalities,
10. investments in training, reskilling and upskilling of CIP professionals so that they can exploit and fully leverage innovative systems, processes and technologies.

Future EU-CIP work will extend this analysis.

On 20-21 September 2023 the EU-CIP consortium held its 1st Annual Conference on Critical Infrastructure Resilience, “Reinventing Resilience”. The conference was held in conjunction with a workshop of the European Cluster for Security Critical Infrastructures (ECSI), and included representatives of European critical infrastructures, researchers, and security solution providers. Discussions covered resilience in the present landscape while also evaluating emerging threats and both existing and required solutions. There was a Roundtable Panel that assessed threats, gaps and needs, a Roundtable Panel that assessed current market solutions and practitioners’ needs, and a European Cluster for Security Critical Infrastructures workshop that identified key takeaways and recommendations for future actions. A comprehensive conference report will be issued, but key points presented in the initial press release that relate to needs and challenges [11] were as follows:

- In today's environment, characterized by constant and sometimes extreme pressure on infrastructures, **operators must move beyond mere compliance and prioritise resilience**. Achieving this demands collaborative and multidisciplinary efforts.

[10] EU-CIP Newsletter Number 1; June 2023.
[11] 1st EU-CIP Annual Conference Promotes “Reinventing Resilience” For European Critical Infrastructures; September 29, 2023; https://www.eucip.eu/2023/09/29/1st-eu-cip-annual-conference-promotes-reinventing-resilience-for-european-critical-infrastructures/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101005292

- As the nature of attacks continues to evolve, the skills of operators and security personnel must evolve in tandem. **Skill development is crucial for the future of European resilience**, encompassing both education and practical experience.
- The importance of **procurement in operationalising innovative technologies** to enhance CI resilience.
- The lack of **post (R&I) project investment**, despite many R&I projects producing valuable results for CI resilience.
- Speakers recognized the potential of AI solutions for bolstering resilience, but they also highlighted the malicious use of AI in infrastructure attacks. **Tools for preventing malicious AI usage** or protecting against it are in demand.
- The importance of **breaking down silos and fostering a community-oriented approach** to CIP.
- The significant **impact of AI on critical sectors**, particularly as a tool for anticipating attacks.
- The necessity of **dynamically adapting incident response strategies** to emerging threats.
- **The importance of disseminating project results after their conclusion**, creating a timeline of relevant projects by area and sector, and establishing links between their work.

3.2.2.2 Disaster Resilience Knowledge Network promoting innovation, technology uptake and multi-stakeholder cooperation (DIREKTION)

The objective of the DIREKTION project is to help firefighters, rescuers, emergency medical responders and civil protection staff to implement effective and affordable solutions to support their operations. The DIREKTION project will establish and implement mechanisms and procedures to enhance knowledge sharing by directing the development of innovative technologies to address the needs of practitioners and policymakers. The DIREKTION project is building on the results of the Horizon 2020 Fire and Rescue Innovation Network (FIRE-IN) CSA [12], which developed a network of first responders, researchers, and companies to improve access to new Fire & Rescue technologies. The FIRE-IN project has identified the needs of and challenges faced by the Disaster Resilience community across Europe, and this work will be extended by the DIREKTION project. Key points from the FIRE-IN project are summarised below.

Policy makers face new challenges from crises and disasters that can have a high impact on society, exceeding the capacities of risk and emergency management systems [13]:

- High Flow of resources in a hostile environment scenario
    - A fast arrival, fast deployment and the capacity to sustain efforts over time is key.
    - There is a need to work inside a hostile environment positioning crews in time and place to deploy tactics, and to organize efforts from outside.
    - A bottleneck is to maintain operative effort in time and space.
- High Impact Low Frequency scenarios
    - These events are emergencies that exceed fire/emergency service capacities and have a high impact on the society.
    - As there aren´t enough resources, the ones in place should focus on critical points and key missions. Avoiding the collapse of the emergency system and maintaining the initiative over the emergency is key.

[12] Fire and Rescue Innovation Network; https://cordis.europa.eu/project/id/740575
[13] FIRE-IN Deliverable 1.4. Report on current and future common capability challenges #3; January 2021.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

- Low Frequency means very few opportunities to acquire and maintain the needed expertise. Fragmentation of fire/emergency services reduces expertise.
- A bottleneck is to develop appropriate capabilities in fire/emergency services and in the society.

- Multi-agency/ Multi-leadership scenarios
  - There are often multiple decision-makers/ leaderships at different levels and from various agencies, with overlapping competences. Sometimes there are also unknown and unclear stakeholders.
  - There is complex integration of interests, decision-making levels, communication systems, cultures, languages...
  - A bottleneck is to integrate the decision-making in short time at different scales and levels focusing on strategic objectives.

- High Level of Uncertainty scenarios
  - Dynamic, unexpected risks and opportunities are emerging at a high pace due to complex, unpredictable interactions.
  - High flow of new unpredicted risks that overcome the available resources; changes in situations exceed the communication capacity.

The FIRE-IN has project has identified current and future capability challenges of practitioners, defined as Common Capability Challenges (CCCs) and Future Common Capability Challenges (FCCCs), and has identified capability challenges requiring research as a matter of urgency below [14]:

1. Capability challenges requiring research with high urgency
   1) CCC9: Train specific roles and risks and invest in a robust knowledge cycle
   2) CCC11: Build a shared understanding of the emergency, and train interagency scenarios
   3) CCC13: Make operational decisions based on building an understanding of the emergency and its evolution
   4) CCC21: Pre-plan a time-efficient, safe response, minimizing responder's engagement
   5) CCC22: Plan in a more integral way
   6) FCCC4: Strategic management focused on proactively reducing sources of uncertainty and building robustness and resiliency
   7) FCCC12: Focus on capacity building towards more resilient societies
   8) FCCC23: Pre-plan interoperability and enhance synergies
2. Capability challenges requiring research with urgency
   1) CCC1: Organize to sustain safe operations
   2) CCC2: Anticipate and prioritize avoiding the collapse of the emergency system
   3) FCCC8: Cultural change towards risk tolerance and resilience
   4) FCCC10: Fire and Rescue (F&R) services empowered to innovate and build organizational learning
   5) FCCC19: Integrate risk prevention and safety into other policies and actors

[14] FIRE-IN Deliverable D3.7. Final Strategic Research and Standardisation Agenda; .

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

6) FCCC16: Create certainty and shared vision of emergencies

7) FCCC20: Focus on governance and integral risk management (for risk reduction).

8) FCCC24: Focus on governance and integral risk management (for preparedness).

The FIRE-IN project has also made R&D recommendations on technology, materials, equipment and facilities in the final strategic research and standardisation agenda [15], as below:

- Specific technologies have been identified as being of high importance:
    - **Early warning technologies** are in high demand, together with **crowdsourcing applications, GIS and geolocation systems, and risk assessment applications**, and future EU R&D should aim at improving and innovating solutions in this area.
    - **Gamification and simulation tools** (computer-based or in the field) are crucial for training first responders.
- Need to improve innovation procurement procedures and reduce costs and bureaucracy in the acquisition of new technologies.
    - New technologies for first responders and civil protection agencies are being adopted but the rate of adopting new technologies is slow.
    - Some new innovations fail to reach full maturity (TRL7/8) due to lack of funding for advanced development ('valley of death').
    - Some practitioners are risk-averse and prefer to rely on familiar technologies with which they are confident or on specific providers with which they are familiar.
    - Another problem is the variety of procurement processes in different stakeholder organisations with some procurements down to municipal/ local level, making the financial return from R&D, particularly for SMEs, too low to justify investment.
    - Some technologies are becoming increasingly expensive discouraging first responder organisations' from procuring them.
- The equipment and technologies should cover a variety of hostile environments.
- The collaboration of industry and academia/research with first responders and practitioners in general can help substantially in the development of new products.
    - Manufacturers and technology providers should be able to demonstrate the capabilities of their solutions and technologies during exercises, trials, workshops, shows organized by fire protection and rescue/ emergency services and scientific units etc.
    - The fire protection and rescue/ emergency services community should be made aware of the existence of new technologies and the opportunities they offer.
- Technology is a supportive tool but the proper use of technology requires testing, competence centres, networking and coordination and suitable facilities for training in hostile environments.

3.2.2.3 European Network Against Crime and Terrorism (ENACT) and EU Terrorism Situation and Trend Report

The objective of the ENACT project is to set up a Knowledge Network in the Fighting Crime and Terrorism (FCT) area capable of i) supporting the EU-funded FCT security R&I cycle and the overall community and market actors with actionable evidence, and ii) boosting the Innovation uptake of the outcomes and results stemming from FCT

[15] FIRE-IN Deliverable D3.7. Final Strategic Research and Standardisation Agenda; November 2022.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Security funded R&I projects. The ENACT project has not yet published public information on practitioner needs and challenges but future outputs will be reviewed in the Secur-IT project.

However there are useful insights on Crime and Terrorism needs and challenges from Europol's annual EU Terrorism Situation and Trend Report (TE-SAT) 2023[16], which has identified how digital and technological advancements are being exploited by terrorists and violent extremists for recruitment, dissemination of propaganda and operations. This poses the following challenges for law enforcement counter terrorism:

- **Encrypted instant communication applications:** Openly available instant messaging applications facilitate communication within terrorist and violent extremist communities. Their end-to-end encryption functionalities continue to pose a challenge to law enforcement authorities in identifying and removing terrorist and violent extremist content online.
- **Gaming platforms:** Terrorist and violent extremist groups and individuals continue to exploit gaming-adjacent platforms for recruitment purposes and propaganda dissemination. IS supporters for example created groups on gaming communication apps, dedicated to the discussion of different topics, including media operations, translation of propaganda content and religious migration.
- **Decentralised technologies:** Jihadist and right-wing propagandists have consolidated their presence on decentralised applications. Using peer-to-peer (P2P) network protocols rather than centralised infrastructures, decentralised technologies pose a serious challenge to content moderation and investigative efforts. Decentralised platforms have multiple options for privacy leading to near-anonymity, enhanced usability, and increased availability and retrievability of on-demand content. These features support the online communication and distribution strategies of both jihadist and violent right-wing propagandists.
- **3D-printed weapons:** The manufacture and use of 3D-printed weapons have already been observed, mainly in the right-wing terrorist and extremist scene.
- **Virtual financial technologies:** The use of financial technologies has also had an impact on the financial activities of terrorist and violent extremist groups and is likely to further transform terrorism financing. Some terrorist and extremist elements have been increasingly using Virtual Assets, especially cryptocurrencies, which provide higher levels of anonymity, in order to finance their terrorist activities.

3.3 Gap Results and Conclusions

Gaps in Cyber Physical Security capabilities, technologies etc that could be addressed by investment or other action have been identified in other EU supported policy development activities covering Cybersecurity, Critical Infrastructure Protection (CIP), Disaster Resilient Societies (DRS) and the Fight against Crime and Terrorism (FCT - which includes public space protection) as follows:

- **Cybersecurity** - European Commission 'Cybersecurity cOmpeteNCe fOr Research anD InnovAtion' (CONCORDIA) CSA project;
- **Critical Infrastructure Protection** (CIP) - European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection (EU-CIP);
- **Disaster Resilient Societies** (DRS) – Disaster Resilience Knowledge Network (DIREKTION);
- **The Fight against Crime and Terrorism** (FCT) - EU Terrorism Situation and Trend Report 2023. This domain covers Public Space Protection (addressed in SecurIT).

These gaps are summarised below in Table 11 and combined with the main gaps identified by SecurIT in its project funding and support activities to identify cross-cutting issues.

[16] EU Terrorism Situation & Trend Report (TE-SAT) 2023: Reviewing the terrorism phenomenon; 14 Jun 2023.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Table 11 – SecurIT and other EU Actions Gap Summary

Source	CONCORDIA	EU-CIP	FIRE-IN/ DIREKTION	EU Terrorism Situation and Trend Report 2023	SecurIT Analysis Results
Category	CSA	CSA	CSAs	Report	Innosup
Cyber Physical Security Activities covered	Cybersecurity	Critical Infrastructure Protection	Disaster Resilience	Fight against Crime and Terrorism	Sensitive infrastructure protection Disaster Resilience Public Spaces Protection
Gaps/ needs	Technology stack recommendations are: 1) Digital twins and possible safety impact; 2) Protect the AI models, engines, and data pipelines from manipulations; 3) Protect against AI weaponized threats; 4) Protection against deepfake.	CIP capability gaps/ needs are: 1) Enhanced adaptability; 2) Reduced response times; 3) Increased transparency of CIP solutions; 4) Improved detection capabilities based on advanced analytics; 5) Improved risk assessment capabilities to address asymmetric and hybrid threats,; 6) capabilities addressing cascading effects across interconnected infrastructures; 7) support for proactive identification of threats based on real-time functions; 8) automated situation awareness based on multi-sensor inputs; 9) Risk prediction functionalities; 10) Investments in training, reskilling and upskilling of CIP professionals. 11) Malicious use of AI in infrastructure attacks. 12) Need to use AI as a tool for anticipating attacks.	High impact challenges from crises and disasters are: 1) Organising rapid flow of resources into and sustained deployment within a hostile environment scenario. 2) High Impact Low Frequency scenarios exceeding response capacities with few opportunities to acquire and maintain necessary expertise. 3) Multi-agency/ Multi-leadership scenarios requiring complex integration of decision-making, communication systems, etc. 4) High Level of Uncertainty scenarios with rapid flow of new unpredicted risks that stress resources and exceed the communication capacity. Key technologies: 1) Early warning technologies together with crowdsourcing applications, GIS and geolocation systems, and risk assessment applications. 2) Gamification and simulation tools (computer-based or in the field) are crucial for training first responders.	Law enforcement counter terrorism challenges are: 1) Encrypted instant communication applications. 2) Exploitation of gaming platforms by terrorist and violent extremist groups. 3) Decentralised technologies for online communication by terrorist and violent extremist groups. 4) Manufacture and use of 3D-printed weapons. 5) Virtual financial technologies for anonymous terrorist and violent extremist group financing.	SME solution application gaps are: 1) Disaster resilience - Optimisation of communication and warning systems in case of disaster. 2) Disaster resilience - Development of solutions for a better recovery. 3) Public Spaces Protection - Communication networks and post-event analysis. SME business case/ technology gap: 1) Limited use of Quantum Technologies. Other SME gaps: 1) regulation, 2) end user understanding, 3) collaborations, 4) slow innovation adoption, 5) finance.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

The gaps identified above fall into two categories, technology development needs that have relevance across domains and domain specific requirements that are being addressed by domain stakeholders and are not considered further.

Analysis of these gaps between supply and demand has identified fifteen **Cross-cutting Technology Development Gaps/ Needs** with relevance across the **Cybersecurity, Critical Infrastructure Protection, Disaster Resilient Societies and the Fight against Crime and Terrorism domains** (making the business case more attractive e.g. Digital twin safety is a Cybersecurity and Critical Infrastructure Protection issue, Multi-agency/ multi-leadership scenarios are relevant to Disaster Resilience and Critical Infrastructure Protection) where innovation is needed, providing opportunities for SMEs, as below:

1) Digital twins and possible safety impact (highlighted by CONCORDIA).

2) Protect the AI models, engines, and data pipelines from manipulations (highlighted by CONCORDIA, EU-CIP)).

3) Protect against AI weaponized threats (highlighted by CONCORDIA).

4) Protection against deepfake (highlighted by CONCORDIA).

5) Improved risk assessment capabilities to address asymmetric and hybrid threats (highlighted by EU-CIP);

6) Need to use AI as a tool for anticipating attacks (highlighted by EU-CIP).

7) Command and Control and Training capabilities to organise rapid flow of resources into and sustained deployment within a hostile environment scenario (highlighted by DIREKTION).

8) Training capabilities to prepare for High Impact Low Frequency scenarios exceeding response capacities with few opportunities to acquire and maintain necessary expertise (highlighted by DIREKTION).

9) Command and Control and Training capabilities to manage Multi-agency/ Multi-leadership scenarios requiring complex integration of decision-making, communication systems, etc (highlighted by DIREKTION).

10) Command and Control and Training capabilities to manage High Level of Uncertainty scenarios with rapid flow of new unpredicted risks that stress resources and exceed the communication capacity (highlighted by DIREKTION).

11) Tools to counter the use of gaming platforms and decentralised technologies for online communication by terrorist and violent extremist groups (highlighted by EU Terrorism Situation and Trend Report 2023).

12) Technologies to counter the manufacture and use of 3D-printed weapons (highlighted by EU Terrorism Situation and Trend Report 2023).

13) Disaster resilience - Optimisation of communication and warning systems in case of disaster (SecurIT user need SMEs found it challenging to respond to).

14) Disaster resilience - Development of solutions for a better recovery (SecurIT user need SMEs found it challenging to respond to).

15) Public Spaces Protection (Public Events) - Command and control (resource management) and decision-making support: Communication networks and post-event analysis (SecurIT user need SMEs found it challenging to respond to).

Looking across the results, the main theme that emerges is that while EU SMEs are adopting most emerging technologies well, as shown in the high level of use of AI and Machine Learning technologies in SME SecurIT cybersecurity and physical surveillance proposals, bad actors are adopting these new technologies just as quickly

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

if not faster and using them to pose significant security threats. SMEs should be able to respond quite quickly to new threats provided there is a business case for them to do so.

Using a project clustering approach (Section 2.4) to enable SMEs with solutions (or components of solutions) to counter emerging technology threats, to interact with end-users from different domains and MS with access to funding, offers a possible approach to accelerate adoption of SME solutions to such threats.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

4. CONCLUSIONS AND RECOMMENDATIONS

SecurIT has published a **Repository of Security and Cybersecurity Requirements** that presents common gaps and needs identified by security practitioners that offer opportunities for SME innovations and address security threats to citizens. Annex 2 presents the final version of the challenges as used in Open Call 2. See Section 2.2.

While the SecurIT-project provided maybe only minor in collating and relating to some of the challenges identified by research and users in terms of needs and requirements identified; both the gap analysis and the analysis of the Open Call activities indicated that the Open Call activities and innovation funding, when focused can contribute quite significantly to innovation, to resolving challenges and bridging gaps. The industry, especially with SMEs, is quite capable in addressing – but also identifying gaps, and more importantly working along closely with the challengers to fullfill their needs.

> **Recommendation 1 – Targeted but SME-supporting innovation funds such as the SecurIT project contribute directly to the needs and requirements, existing market gaps. It is recommended to policy makers both on European and regional level to continue expanding these creativity support programs as they support both SMEs, innovation and end users such as law enforcement, critical infrastructures and security end users.**
>
> **Recommendation 2 – It is recommended that the SecurIT Repository of Security and Cybersecurity Requirements is used by policy makers to guide future EU calls for innovation proposals in Sensitive Infrastructure Protection, Disaster Resilience and Public Space Protection (Major Events).**

The 166 security products/services mapped and promoted on the SecurIT online platform (as of June 14th 2024) represents a high proportion of the solutions offered in 241 proposals into the Open Calls, and **significantly exceeds the SecurIT target outcome of generating at least 50 innovative SME solutions to address user needs.** See Section 2.3.

The 166 security products/services mapped and promoted on the SecurIT online platform address all of the challenges identified by SecurIT (Section 2.3) if one considers the core and secondary challenges they address. The highest number of solutions (97) addresses Cybersecurity for Sensitive Infrastructure Protection (Challenge 1.1) while the lowest number of solutions is for Communication and Warning Systems during a crisis (Challenge 2.2).

The main **SME barriers and challenges** identified (Section 2.4) were:

- Regulation - Difficulties in keeping pace with the complex and changing regulatory environment.
- End user understanding - Lack of understanding of end-user needs, requirements, and priorities by SMEs.
- Collaboration building - Challenges maintaining and establishing new collaborations with relevant stakeholders.
- Slow innovation adoption - Very long innovation adoption times by end user organization that are longer than anticipated sales cycles.
- Finance - Financial restraints and limited access to financial instruments.

A **project clustering approach** (Section 2.4) that enables SMEs to interact with end-users from various domains and MS obtaining instant feedback on the relevance of their solutions, while simultaneously presenting end-users with a wide array of innovative technologies tailored to their specific areas of interest, which they can select from, benefits both users and SME suppliers. Use of different national funding instruments for joint development of innovations can also be a very important factor of potential success.

SecurIT has identified the potential benefits of developing an **online tool to make it easier for SMEs to access different level funding instruments** at regional, national and EU level (Section 2.4). Such a tool can help SMEs and SME consortia access cross-border funding sources and help SMEs to scale their security solutions. A prototype (Regional Invest) has been demonstrated to potential stakeholders, but a mechanism would need to be found to support the maintenance of such a system.

> **Recommendation 3 - It is recommended that consideration is given to developing a pan-EU online funding tool to make it easier for SMEs to access funding instruments at regional, national and EU level and help SMEs to scale their security solutions.**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

For both Open Calls **SME bidders were more comfortable bidding into the Secure Infrastructure Protection domain (55% of bids) than Disaster resilience (21% of bids) or Public Spaces Protection (21% of bids)**, either because they were more familiar with the secure infrastructure domain or their capabilities were more suited to it. See Section 2.5.

All eleven user security challenges being addressed by SecurIT have been met by at least one funded solution in Open Call 1 or Open Call 2 that addressed that challenge as its primary (core) challenge (Section 2.5). If one takes secondary (other) challenges into account the funded SecurIT portfolio of bids addresses all of the challenges with at least six solutions, either as core or secondary applications of the funded solutions.

SMEs made substantial use of important technologies, in particular Cybersecurity technologies (detection, biometrics etc) technologies (49% of bids), Artificial Intelligence and Machine Learning system technologies (44%) and Situational Awareness, Surveillance and Sensors technologies (39%) to address the SecurIT challenges (Section 2.5). **AI/ Machine Learning was used extensively by SMEs when solving Cybersecurity and Physical Surveillance challenges.**

Gaps in Cyber Physical Security capabilities, technologies etc that could be addressed by investment or other action have been identified in SecurIT (Section 2.6) and other EU supported policy development activities (see Section 3.2) covering Cybersecurity, Critical Infrastructure Protection (CIP), Disaster Resilient Societies (DRS) and the Fight against Crime and Terrorism (FCT - which includes public space protection) as follows:

1. **Cybersecurity** - European Commission 'Cybersecurity cOmpeteNCe fOr Research anD InnovAtion' (CONCORDIA) CSA project;
2. **Critical Infrastructure Protection** (CIP) - European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection (EU-CIP);
3. **Disaster Resilient Societies** (DRS) – Disaster Resilience Knowledge Network (DIREKTION);
4. **The Fight against Crime and Terrorism** (FCT) - EU Terrorism Situation and Trend Report 2023;
5. **SecurIT** Innosup project (Sensitive Infrastructure Protection, Disaster Resilience and Public Space Protection (Major Events)).

Analysis of these gaps between supply and demand has identified fifteen **Cross-cutting Technology Development Gaps/ Needs** with relevance across the **Cybersecurity, Critical Infrastructure Protection, Disaster Resilient Societies and the Fight against Crime and Terrorism domains** (making the business case more attractive) where innovation is needed, providing opportunities for SMEs, as below:

1) Digital twins and possible safety impact (highlighted by CONCORDIA).

2) Protect the AI models, engines, and data pipelines from manipulations (highlighted by CONCORDIA, EU-CIP)).

3) Protect against AI weaponized threats (highlighted by CONCORDIA).

4) Protection against deepfake (highlighted by CONCORDIA).

5) Improved risk assessment capabilities to address asymmetric and hybrid threats (highlighted by EU-CIP);

6) Need to use AI as a tool for anticipating attacks (highlighted by EU-CIP).

7) Command and Control and Training capabilities to organise rapid flow of resources into and sustained deployment within a hostile environment scenario (highlighted by DIREKTION).

8) Training capabilities to prepare for High Impact Low Frequency scenarios exceeding response capacities with few opportunities to acquire and maintain necessary expertise (highlighted by DIREKTION).

9) Command and Control and Training capabilities to manage Multi-agency/ Multi-leadership scenarios requiring complex integration of decision-making, communication systems, etc (highlighted by DIREKTION).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

10) Command and Control and Training capabilities to manage High Level of Uncertainty scenarios with rapid flow of new unpredicted risks that stress resources and exceed the communication capacity (highlighted by DIREKTION).

11) Tools to counter the use of gaming platforms and decentralised technologies for online communication by terrorist and violent extremist groups (highlighted by EU Terrorism Situation and Trend Report 2023).

12) Technologies to counter the manufacture and use of 3D-printed weapons (highlighted by EU Terrorism Situation and Trend Report 2023).

13) Disaster resilience - Optimisation of communication and warning systems in case of disaster (SecurIT user need SMEs found it challenging to respond to).

14) Disaster resilience - Development of solutions for a better recovery (SecurIT user need SMEs found it challenging to respond to).

15) Public Spaces Protection (Public Events) - Command and control (resource management) and decision-making support: Communication networks and post-event analysis (SecurIT user need SMEs found it challenging to respond to).

Recommendation 4 - It is recommended that the fifteen Cross-cutting Technology Development Gaps/ Needs identified from the results of SecurIT and other EU supported policy development projects, covering the Cybersecurity, Critical Infrastructure Protection, Disaster Resilient Societies and Fight against Crime and Terrorism domains, are considered as SME innovation topics for research agendas by EU policy makers.

Looking across the results, the main theme that emerges is that while EU SMEs are adopting most emerging technologies well, as shown in the high level of use of AI and Machine Learning technologies in SME SecurIT cybersecurity and physical surveillance proposals, bad actors are adopting these new technologies just as quickly if not faster and using them to pose significant security threats. SMEs should be able to respond quite quickly to new threats provided there is a business case for them to do so.

Recommendation 5 - It is recommended that EU policy makers consider using a project clustering approach (as used in SecurIT and described in Section 2.4) to enable SMEs (with solutions or components of solutions to counter emerging technology threats) to interact with end-users (from different domains and MS with access to funding), to help accelerate adoption of SME solutions to address emerging technology threats.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

ANNEX 1 – DATA SOURCES AND TAXONOMIES

DATA SOURCES

The following sources have provided useful insights to supplement the SecurIT work:

- Cybersecurity Industry and Market Analysis in Europe (CIMA) Report 2019
- Deloitte/ ECORYS 2022 EU Security market study for EC (May 2022)
    - Security Areas etc
- ECCO Market Observatory and CIMA Database including preliminary EU market analysis
- ENISA Threat Landscape 2022
- European Cybersecurity Investment Platform and 2022 Report
- European Investment Bank (Website/ Reports)
- Industrial Leadership in Enabling and Industrial Technologies – ICT – Pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research and & Innovation Roadmap: outcomes of SPARTA, ECHO, CONCORDIA and CyberSec4Europe
- JRC ATLAS Database
- Mordor, CYBERSECURITY MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2023 - 2028)
- UK, HMG National Risk Register, 2023 edition

TAXONOMIES USED FOR ANALYSIS

Analysing gaps requires careful use of agreed taxonomies. The following taxonomies have been considered for the analysis:

- Deloitte/ Ecorys EC Study 2022 Security functions/ applications e.g. Data, information & intelligence gathering management, and exploitation; Security of information systems, networks and hardware; Physical access control (of locations, goods, etc.).
- ECSO Taxonomy (linked to NIST Taxonomy)
    - Cybersecurity e.g. IDENTIFY
    - Cyber Physical Services e.g. Audit, planning and advisory services
    - Other Security Products and Solutions e.g. Observation and surveillance (wide area)
- ENISA draft taxonomy for ICT products for EU Cybersecurity Certification (EUCC) scheme (2021) [17]
    - Sectors particularly challenging for the security of ICT products and systems (including areas where future developments can bring new security challenges) e.g. Artificial intelligence and Machine Learning systems, Radio technologies (e.g. 5G Networks , Short dedicated range communications), Cloud, Edge and Virtualization.
- JRC Taxonomy
    - Research Domains e.g. Assurance, Audit, and Certification.
    - End User Sectors e.g. Energy.
    - Technologies used across multiple sectors e.g. Artificial intelligence, Big Data, Blockchain and Distributed Ledger Technology (DLT).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

ANNEX 2 – SECURIT – REPOSITORY OF SECURITY AND CYBERSECURITY REQUIREMENTS

The challenges and potential areas of need, as updated for the second Open Call of the SecurIT project, are defined around 3 main **domains** as, described below, together with examples to illustrate the types of potential **solutions** for applicants captured in a Table of Challenges. These results are taken from Deliverable D2.2 which also describes the process used to produce this repository.

Domain #1: Sensitive infrastructure protection

Sensitive infrastructure protection pertains to the securing of assets and systems that are essential for the functioning of a society and economy. Examples include the provision of gas and oil, agriculture, and telecommunication. The security of sensitive infrastructure is a major concern, confirmed by recent events, in the context of social unrest, terrorist threats and even a pandemic. If this type of infrastructure is exposed to external threats, this will have major consequences for society as a whole. The solutions should address hybrid threats, permit to enhance capabilities, and consider the increasingly interconnected, complex and interdependent networks and systems.

Targeted end-users: for example, end-users of projects around sensitive infrastructure protection include the safety director of vital importance and Seveso classified industrial facilities, airports, hospital infrastructure, energy suppliers, and operators (e.g. electricity, gas, telecommunications, etc.).
Solutions: The solutions developed in this domain will have to integrate the following considerations: maintainability, acceptable price, foresight scanning, and interoperability with existing solutions.

Domain #2 - Disaster resilience

There is a need for instruments that facilitate improved prevention and preparedness in crises, extreme events and natural disasters. In this second focus area of SecurIT, the solutions should focus on development of technologies to strengthen the capacities of first and second responders in all operational phases, and where relevant, to increase societal resilience towards and for citizens. Innovative technologies can help detect, analyse, treat, and/or prevent major natural events. This domain focuses on climate-related risks and extreme events, geological disasters such as wildfires, earthquakes, tsunamis, and pandemics, but also accidental disasters and human-induced disasters (food safety, industrial accidents, infrastructure failures, nuclear accidents, and others).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Targeted end-users: For example, first responders, cities and territories, and their governmental structures.

Solutions: The solutions developed under this domain will have to consider citizen involvement and acceptation and transparency. All solutions will also have to ensure the continuity of operations.

Domain #3 – Protection of public spaces

The objective of this domain is to develop innovative tools that create increasingly connected and protected cities in which the population takes on a more active role in serving the community. These solutions should integrate and consider state-of-the-art technologies like in Artificial Intelligence, Cloud computing, and Big Data.

Targeted end-users: for example, cities and territories (security of public roads), and venues open to the public (e.g.: stadiums; concert zone, train stations, etc.).

Solutions: The solutions developed in this domain will have to consider the legal constraints of personal data protection.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Tables of challenges to be addressed

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #1: sensitive infrastructure protection	**Cybersecurity**	**1.1**	**Development of cybersecurity solutions for sensitive infrastructure protection**	To propose effective cybersecurity solutions and solutions to increase resilience against cyber-attacks: - Cybersecurity of information and communication systems; Data protection and security of data; electromagnetic protection; - Cyber Security incident management; - Cybersecurity - Automatic attack detection and remediation; - Quantum - Post Quantum; - Security Bill of Materials - Device - IoT Security - Shared Responsibility; - Secure Sovereign Cloud.
	Operations	**1.2**	**Optimisation of communication networks and alert systems**	To optimize solutions for better communication networks (assess, detect and alert both operational forces, LEA or emergency services), the hyper vision and command systems and alert systems.
	Identification and access control	**1.3**	**Development and optimization of identification and access control for rapid access in the site, all while ensuring that no one and nothing that enters poses a security risk**	To propose digital innovative solutions to identify, provide entry for and inspect individuals, vehicles and goods requesting access to the site such as: - Access control for people; - Biometrics & multi biometric systems; - Vehicle control & inspection; - Detecting weapons & explosives: stationary or mobile illicit materials like CBRNE (chemical, biological, radiological, nuclear and explosives) and weapons.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Tables of challenges to be addressed

	Zone security and perimeter protection	**1.4**	**Development of solutions to detect and locate any intruders that have managed to penetrate the perimeter protection and barriers to block intrusions**	To propose digital innovative solutions such as: - Data sensors: detectors; system status indicators; IoT; - Video analysis & sensor fusion: deep learning; - Surveillance – Essential components of the decision-making chain are the detection, recognition and identification of land/air/sea vessels and intruders near or inside the protected area – e.g.: optronic solutions; radar sensors; solutions and data processing/analysis software; video protection (embedded AI); - Surveillance Robots: patrol rounds and missions - detection/identification/neutralization of malicious drone; - Securing physical access routes through digital solutions and development of physical access control solutions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Tables of challenges to be addressed

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #2 - Disaster resilience	**Prior to crisis – prediction: Risk knowledge and evaluation**	**2.1**	**Optimisation of prediction of disaster**	To propose innovative solutions and technologies for prevention to: - Enhance exploitation of monitoring data and satellite/remote sensing information as well as artificial intelligence to improve high-level assessment - Production and processing of data by satellite and aerial imagery (UAV/UAS and light aircraft), as well as by sensor networks. This allows for knowledge about areas concerned and potential risks, integrating data about weather and water courses, providing operational maps for decision-makers and rescue managers. - Modelling and geographical information systems: Modelling territories and the simulation of phenomena allow for the substitution of rarely accessible situations by virtual situations in realistic and operational 3D.
	During the crisis: Mass communication and warning systems	**2.2**	**Optimisation of communication and warning systems in case of disaster**	These communication systems must be easily transportable and easily deployable within a timeframe compatible with operational demands. The requirement is to have means of communication, which are suitable, diversified, and interoperable such as: - Technology that enables the management and monitoring of communication from news media, social media, and internal communication sources in a crisis situation - Information vs decision with the support of AI To propose innovative solutions and technologies for disaster response to improve forecast / early warning systems, advanced data management, Information update.
	After the crisis: Post event analysis and recovery	**2.3**	**Development of solutions for a better recovery**	To propose innovation solutions and technologies for post crisis and disaster recovery: - Robotics to carry out tasks in hazardous areas for humans - UAV/UAS can view an « area of interest » and give a good understanding of the environment and the situation in the area affected by a disaster - Energy and data network rehabilitation, autonomous and decentralized – to ensure the conservation of the security of data in the context of post-disaster.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

Tables of challenges to be addressed

	Sub-domains	N°	Challenges and potential areas of needs	Examples and illustrations for applicants
Domain #3 - Public spaces protection – major events	**Detection, alert and behaviour analysis**	**3.1**	**Gather and manage real time information**	To propose innovative solutions for data and information gathering, exploitation and exchange, surveillance and intelligence: facial, speech, and vehicle recognition; CCTVS & cameras (e.g.: embedded AI for flow detection and crowd surveillance, smart cameras, etc.), signal jamming devices for drones, wave scanners systems and anomaly detection systems. To propose warning systems such as innovative tools for public and/or geolocation of public and rescue team.
	Analysis	**3.2**	**Analyse and extract pertinent and potentially crucial information as quickly as possible**	To propose innovative tools that can be used in real-time mode (alert, surveillance, or intervention) or in delayed mode (intelligence, investigations, e.g.: audio analytics systems, SOP updates, blind-spot mapping, performance analyses and determining training programmes etc.). To propose innovative analysis tools to support the responsible authorities in monitoring the public information space and quickly identifying disinformation threats, using emerging solutions for integration of information from multiple and non-traditional sources (e.g., social media) into incident command operations.
	Command and control (resource management) and decision- making support	**3.3**	**Communication networks and post-event analysis**	To produce innovative safe tools that support event planning and resource management during the event. Such tool should support: - connectivity of different authentication level users; - definition of environment (defining time, uploading geo information, defining roles, etc.); - possibility to see location of resources and communicate with all linked entities directly via safe tool; - possibility to provide visual guidance; - possibility to upload new relevant data and share with respective entities; possibility to manage few events at a time. To propose innovative solutions for secure and better public communication and networks, post event analysis, data/information exchange.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292

	Data protection and cybersecurity - cybercrime	**3.4 Detection**	To propose innovation solutions such as: - AI manipulated content analysis: deep fake video detection; deep fake audio detection - Methods for identifying information sources / provenance of information: detection of similar information appearing in different venues / platforms; attribution of information to a single source - Media forensics: image forensics (content manipulation detection; copy-move, splicing, inpainting, enhancement) - Video forensics (content manipulation detection; traditional cut, delete, paste attacks, copy-move, splicing, inpainting, enhancement); audio forensics (content manipulation detection, traditional cut, delete, paste attacks) - Textual content analysis: Image content analysis; Audio content analysis; Video content analysis - Security bills of materials device IoT security shared responsibility.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101005292