



7SHIELD

---

## D8.9 Final networking report

<b>Work Package:</b>	WP8		
<b>Lead partner:</b>	SERCO		
<b>Author(s):</b>	Adriana Grazia Castriotta (SERCO), Barbara Scarda (SERCO), Franck Ranera (SERCO)		
<b>Due date:</b>	January 2023		
<b>Version number:</b>	1.0	<b>Status:</b>	Final
<b>Dissemination level:</b>	PU		

---

<b>Project Number:</b>	883284	<b>Project Acronym:</b>	7SHIELD
<b>Project Title:</b>	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats		
<b>Start date:</b>	September 1 <sup>st</sup> , 2020		
<b>Duration:</b>	30 months		
<b>Call identifier:</b>	H2020-SU-INFRA-2019		
<b>Topic:</b>	SU-INFRA01-2018-2019-2020 Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe		
<b>Instrument:</b>	IA		

---

## Revision History

Revision	Date	Who	Description
0.1	22/12/2022	SERCO	First release of the table of content
0.2	10/01/2023	SERCO	First version of the document
0.3	27/01/2023	CS, SPACEAPPS	Internal peer review's results
0.4	30/01/2023	SERCO	Final version including formatting remarks received by the internal reviewers
1.0	31/01/2023	ENG	Version ready to be submitted in EC portal

## Quality Control

Role	Date	Who	Approved/Comment
Internal review	24/01/2023	CS	<i>Approved - minor formatting remarks</i>
Internal review	27/01/2023	SPACEAPPS	<i>Approved - minor formatting remarks</i>

## Disclaimer

This document has been produced in the context of the 7SHIELD Project. The 7SHIELD project is part of the European Community's Horizon 2020 Program for research and development and is as such funded by the European Commission. All information in this document is provided 'as is' and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view.

## Executive Summary

---

The main objective of Task 8.2 – Collaboration, clustering and networking activities is to raise awareness of the project by disseminating its activities and results among key stakeholders, practitioners and researchers, with the ultimate goal of establishing useful connections for possible synergies. This document reports the activities to achieve such objective, describing the results of the following activities to involve key stakeholders, practitioners, and researchers to a network of interest:

- (1) **participation of partners in targeted international external events** (workshops, conferences and exhibitions) and the establishment of relevant networking activities;
- (2) initiate **broad and continuous dialogue within project members and other stakeholders** to guide implementation and evolution of security frameworks in the Ground Segment domain;
- (3) collate information and experiences (i) to benefit from other projects' outcomes, methodologies, best practices and success stories, (ii) to **foster clustering between associated beneficiaries of the H2020**, (iii) to identify opportunities for further collaboration and (iv) to perform profitable and fruitful collaborations.

It is worth to be mentioned that, especially during the first 2 years of the project, most of the events were organised virtually, and this had a negative impact on the success of individual networking. However, at the same time, the ability to attend more virtual events also increased, as did the possibility to reach broader audiences with dissemination activities.

A total of 39 unique international external events were attended by the 7SHIELD partners throughout the project lifetime and the average attendance is in line with the initial expectation that each partner participates in at least 2 events. The identified events engaged various types of audiences, including sector-specific professionals in the domains of Space Industry, Earth Observation, Remote Sensing, Critical Infrastructure, Security, Crisis Management, so as to include the maximum possible range of interested parties. Dissemination activities as well as individual interactions during the events have been both key elements to promote the project and building a network of contacts.

Once the network of contacts was built and members were engaged, 7SHIELD tried to create a strong feeling of community among the different stakeholders around the same objectives to promote exchanges and interactions. A total of 71 internal workshops were organised in coordination with project partners with the aim of collecting feedback and improvements and create value for the project. Approaching the conclusion of the project, on 14 December 2022, a tailored **7SHIELD Info Day** was organized in Brussels in hybrid format (in presence and online) engaging publicly the participation of external stakeholders.

The objectives of the event were to describe the achievements of the project, show the results that were obtained in real conditions through the five 7SHIELD's Space Ground Segments acting as Pilot Use Cases, and raise the interest in the value and exportability of the 7SHIELD tools and solutions in different contexts.

The agenda of the Info Day was purposely conceived as a series of interactive sessions requiring the active involvement of participants and allowing intercommunication among the attendees. A special focus was also given to the 20 Key Results that were discussed and presented throughout the day.

104 persons were registered to the event, including 38 external stakeholders, with an 80% rate of attendance and 60% of them participated in presence.

Furthermore, during the project lifetime, clustering activities took place with the objectives to collect information, to feed project evolution's lines, to stimulate exchange of information but also to challenge technologies and ideas with feedback coming from different sources (end users, industrial stakeholders, etc.). All in all, this activity aimed to build a community of experts in the security of critical infrastructure,

be it physical or cyber, and to feed the vertical and horizontal network to sustain the continuity of the service at project's end.

## Table of Contents

Executive Summary .....	4
1. Introduction.....	10
2. Networking activities.....	11
2.1. Introduction .....	11
2.2. Procedures for tracking external events .....	11
2.3. List of attended external events.....	13
3. Collaboration activities.....	20
3.1. Internal workshops.....	20
3.2. Tailored Info Day.....	22
3.2.1. Sponsor team.....	23
3.2.2. Event co-design.....	27
3.2.3. Communication support .....	29
3.2.4. Organization of the event.....	30
3.2.5. 7SHIELD Info Day Event .....	34
3.2.6. Follow-up.....	40
4. Clustering activities.....	42
4.1. DroneWISE H2020 project .....	42
4.2. European Cluster for Securing Critical Infrastructure (ECSCI) .....	43
4.3. EU-HYBNET .....	43
4.4. CERIS.....	44
4.5. The Security Mission Information and Innovative Group (SMI2G).....	45
5. Conclusions and Future Outlook.....	46
6. References.....	48
Annex I – Results and comments on questionnaires done during the info day .....	49
Annex II – 7 identified thematic areas and the reasons why they are useful in a security framework .....	54
Annex III – Q&A .....	56

## List of figures

Figure 2-1 – 7SHIELD Events list shared file.....	12
Figure 2-2 – Event Promotion template .....	12
Figure 2-3 – Event Report template .....	13
Figure 2-4 – Events – Attendance by Partner.....	17
Figure 2-5 – Events – In-person / Virtual rate.....	17
Figure 2-6 – Events – Type of events.....	18
Figure 2-7 – Events - Type of participation .....	19
Figure 3-1 – Collaboration pillars.....	20
Figure 3-2 – Event set-up and organization.....	22
Figure 3-3 – Individual exercise in order to collect the personal view of the sponsor team on objectives and outcomes of the Info Day .....	24
Figure 3-4 – Collaborative discussion during the sponsor team meetings on the five organization ...	24
Figure 3-5 – Identified themes of the 7SHIELD Info Day by the sponsor team meeting .....	25
Figure 3-6 –7SHIELD Info Day agenda .....	26
Figure 3-7 –Scan-Focus-Act model for event organization, facilitation and execution.....	28
Figure 3-8 – Jamboards for the co-design sessions .....	29
Figure 3-9 –LinkedIn posts for invitation to the Info Day .....	30
Figure 3-10 – Badges, KR and thematic area cards created for the Info Day .....	33
Figure 3-11 – Room setup for presentation sessions and the re-setup of the environment for the interactive session (working groups) .....	34
Figure 3-12 – UAV available during the info day.....	34
Figure 3-13 – Image of the Info Day registration scores.....	35
Figure 3-14 – Image of the organization type of external stakeholders participating to the Info Day .....	35
Figure 3-15 – Image of the participation scores.....	35
Figure 3-16 – Questionnaire, live results and comments .....	37
Figure 3-17 – Presentations in Pecha Kucha style .....	38
Figure 3-18 – Phase 1 of the Session in which 7 working groups identified the reasons why the 7SHIELD thematic areas are important for a security framework .....	39
Figure 3-19 – Phase 2 of the Session in which 7 working groups exposed to the audience the identified reasons why each of the 7SHIELD thematic areas are important for a security framework .....	40
Figure 3-20 – Phase 3 of the info day Session in which the identified 7SHIELD thematic areas are shown in action, by using demonstration videos sorted by extraction of cards and followed by quizzes .....	41
Figure 4-1 – 7SHIELD participation to DroneWISE.....	42
Figure 0-1 – Question 1 .....	49
Figure 0-2 – Question 2 .....	49
Figure 0-3 – Question 3.....	50
Figure 0-4 – Question 4.....	50
Figure 0-5 – Question 5.....	51
Figure 0-6 – Question 6.....	52
Figure 0-7 – Question 7.....	53

## List of Tables

Table 2-1 – List of attended Events.....	14
Table 2-2 – Presentations on specific 7SHIELD topics at external events.....	18
Table 3-1 – Internal workshops and interviews .....	21
Table 3-2 – Event organization steps .....	22
Table 3-3 – 7 thematic areas definition.....	30
Table 3-4 – 7 thematic areas definition.....	31
Table 3-5 – Event tools .....	32
Table 4-1 – 7SHIELD Connections list.....	43





## Definitions and acronyms

CA	Consortium Agreement
CER	Critical Entities Resilience
CERIS	Community for European Research and Innovation for Security
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CoU	Community of Users for Safe, Secure and Resilient Societies
CPS4CIP	Cyber Physical Security for Critical Infrastructures Protection
C/P	Cyber/Physical
DoA	Description of Action
DSS	Decision Support System
EC	European Commission
ECSCI	European Cluster for Securing Critical Infrastructure
EU	European Union
FR	First Responders
GA	Grant Agreement
HRB	Horizon Results Booster
IT	Information Technology
IoT	Internet of the Things
KR	Key Result
MS	Member State
Q&A	Questions and Answers
PC	Project Coordinator
SA	Situation Awareness
SC	Scientific Coordinator
SGS	Satellite Ground Station
SMI2G	Security Mission Information and Innovative Group
TM	Technical Manager
UAV	Unmanned Aerial Vehicle
WP	Work Package

## 1. Introduction

---

This deliverable focuses on all networking, collaboration and clustering activities done in the frame of the WP8 – *Dissemination, Impact Creation and Exploitation Plan* over the duration of the 7SHIELD project. It summarises these activities, reporting some statistical values, and also reflects on achievements in reaching all target project audiences.

The communication and dissemination activities were to some extent affected by the COVID-19 pandemic, which coincided with the first 21 months of the project. This led to a shift in focus to online communication at the expense of physical meetings.

Additional limitations resulted from the impossibility of sharing classified information within EU RESTRICTED documentation between technical partners and communication team which implied the need to create declassified versions of the deliverables and constantly recall, within the project partners, during the videoconference and meetings, that a particular attention on the shared information must be applied in order to not divulgate restricted information.

The **Section 2** of the report contains an overview of **networking** activities connected with 7SHIELD's efforts to communicate with the target groups defined in DoA and in the *D8.1 – Communication and dissemination plan document*. This section provides the methodology for choosing and assign the event participation within partners and provides the list of the project meetings and technical forums/workshops and conferences the partners participated.

The **Section 3** describes the results of the **collaboration** activities to involve key stakeholders (internal and external), practitioners, and researchers to a network of interest, including the organization of a tailored Info Day.

The **Section 4** describes the key **clustering** activities that took place during the project lifetime, with the objectives to collect information, to feed project evolution's lines, to stimulate exchange of information but also to challenge technologies and ideas with feedbacks coming from different sources.

The **Section 5** provides the conclusion and outlook while **Annexes** reports the main results of the 7SHIELD Info Day (collected via questionnaires and working teams) and the Q&A.

## 2. Networking activities

### 2.1. Introduction

The main objective of *Task 8.2 - Collaboration, clustering and networking activities* is to raise awareness of the 7SHIELD project by disseminating its activities and results among key stakeholders, practitioners, policy makers and researchers, with the ultimate goal of establishing useful connections for possible synergies.

The objective has been pursued through the participation of partners in targeted international external events (workshops, conferences and exhibitions) and the establishment of relevant networking activities.

The identified events engaged various types of audiences, including sector-specific professionals in the domains of Space Industry, Earth Observation, Remote Sensing, Critical Infrastructure, Security, Crisis Management, so as to include the maximum possible range of interested parties.

The type of participation of 7SHIELD partners in these external events was also varied, ranging from ordinary participation to presentation and exhibition, allowing therefore different levels of networking possibilities. Dissemination activities as well as individual interactions during the events have been both key elements to promote the project and building a network of contacts.

It is worth to be mentioned that, especially during the first 2 years of the project, most of the events were organised virtually, and this had a negative impact on the success of individual networking. However, at the same time, the ability to attend more virtual events also increased, as did the possibility to reach broader audiences with dissemination activities.

### 2.2. Procedures for tracking external events

In order to maximise participation to external events and to track the outcomes, a series of structured procedures were put in place throughout the project, involving a number of resources:

- “7SHIELD Events list”, a table (as shown in Figure 2-1) listing all upcoming events of interest and shared with all partners. All events relevant to the 7SHIELD topics and targeting specialist audiences identified as key stakeholders that could potentially bring synergies, were mapped on this table, with an active contribution from all the partners. This table was conceived as an internal live document where partners were able to add new events and record their participation.
- Collection of reports from all partners attending external events, as outlined on the “7SHIELD Communication and Dissemination Handbook”, developed as part of Task 8.1.

These reports include:

- a) the pre-event “Event Promotion” (template in Figure 2-2), feeding both the 7SHIELD website in the [Events](#) section and the project [Linkedln page](#) in order to communicate the foreseen participation and involve the interested communities through the posts’ shares and likes.

Input from Partner	Attendee (Partner)	Attendance Confirmed	Type of Participation	Type of Event	Event Title	Event Website	Start Date	End Date	Location	Registration Cost	Abstract deadline
SERCO & CS	SERCO	Yes	Speaker	Conference	PhI Week	<a href="https://phweek.ecpa.org/">https://phweek.ecpa.org/</a>	1-Oct-20	1-Oct-20	Virtual		
SERCO	SERCO	Yes	Speaker	Workshop	Workshop "Leveraging the EU infrastructures in Europe"	<a href="https://www.eurospdr.net/workshops/40-workshop-scaling-sentinel3-europe-online">https://www.eurospdr.net/workshops/40-workshop-scaling-sentinel3-europe-online</a>	19-Oct-20	19-Oct-20	Virtual		
ENG & CS	ENG	Yes	Speaker	Conference	Nicosia Risk Forum 2020	<a href="https://boson.com/events/nicosia-risk-forum-2020">https://boson.com/events/nicosia-risk-forum-2020</a>	28-Nov-20	28-Nov-20	Virtual		
ENG & CS	CS	Yes	Speaker	Conference	Nicosia Risk Forum 2020	<a href="https://boson.com/events/nicosia-risk-forum-2020">https://boson.com/events/nicosia-risk-forum-2020</a>	28-Nov-20	28-Nov-20	Virtual		
ENG	ENG	Yes	Speaker	Conference	2nd Secure Societies "Project to Policy Kick-Off Seminar" (P2PKOS) [MEETING]		22-Mar-21	23-Mar-21			
SPACEAPP	SPACEAPP	Yes	Speaker	Workshop	Teleconference on ESA Ground Segment security policy and standards with DG-X, ESRN		1-Apr-21	1-Apr-21	Virtual		

	M	N	O	P	Q	R	S	T	U	V	W
	Presentation Title	Abstracts / presentation approved by AWC	Attendee (name)	Organizer	Contact	7SHIELD EVENTS	7SHIELD ARTICLE	7SHIELD LinkedIn	Newsletter	Comments (motivation to participate)	Audience Target
2	"ONDA Contribution to DTE"		Franck Ranera	ESA	franco@esa.int	Yes	Yes			Promotion of 7SHIELD project with Kubernetes solution	
3			Franck Ranera	EUSDR						Promotion of 7SHIELD project with Kubernetes solution	
4	General presentation of 7SHIELD project		Gabriele Giunta & Xavier Poitrat	The Minister of Foreign Affairs of the Republic of Cyprus	george.boustras@g.boustras@foc.ac.cy					Presentation and promotion of 7SHIELD project	Risk experts
5	General presentation of 7SHIELD project		Gabriele Giunta & Xavier Poitrat								
6	7SHIELD Policy Brief presented			REA							
7	7SHIELD general presentation and brochure		Leslie Gale	ESA/ESRIN						Present 7SHIELD and discussion on ESA Ground Segment security policy and standards	

Figure 2-1 – 7SHIELD Events list shared file



## EVENT PROMOTION

Event Name:		Event Organiser:	
Location:		Start date / End date:	
Link to the event:			

Name	Company	Role (Speaker/participant)

**Rationale for Participation: Why this event is relevant to 7SHIELD?**

**LinkedIn Post (Max 150 words)**  
*The LinkedIn post should introduce the event (name of the event, organiser, date, location, topic), the participants (7SHIELD partners), and the links to 7SHIELD projects.*

**Corporate presentation of the event**  
*Report here the official presentation of the event*

**Illustration of the event (logo/picture)**  
*Report here the official illustration of the event*

COMMENTS

Figure 2-2 – Event Promotion template

- b) the post-event “Event Report” (template in Figure 2-3), feeding the website with a full article where applicable ([News](#) section) and the [LinkedIn page](#). This report provides feedback on the outcomes of the partners’ attendance to external events, and it also includes a section on “Networks: contacts established” for each partner to fill in, as applicable. Therefore, it is a key element to the collection of the networking activities progress. The contacts recorded by all partners were then used for building the 7SHIELD Info Day invitation list.



## EVENT REPORT

Event Name:		Event Organiser:	
Location:		Start date / End date:	
Number of participants:		Communities of participants:	

Name	Company	Role (Speaker/participant)

Title of your presentation(s) (if any)  
*Please provide in attachment of this report any presentation that can be publicly published*

LinkedIn Post (**Max 150 words**)  
*The LinkedIn post should introduce the event (name of the event, organiser, date, location, topic), the participants (7SHIELD partners), the links to 7SHIELD projects and/or the presentation(s) made by 7SHIELD partner(s) during the event and the potential results of the event.*

Website article (**Min 300 words**)  
*The Website article should introduce the event (name of the event, organiser, date, location, topic), the participants (7SHIELD partners), the links to 7SHIELD projects. The article should go in depth with the event results/ the presentation(s) made by 7SHIELD partner(s) during the event and/or with the technology topics related to the event etc.*

Illustrations of the event (pictures, screenshots etc.)

**NETWORKING: CONTACTS ESTABLISHED**

Name	Position	Contact (mail, phone...)

**COMMENTS**

Figure 2-3 – Event Report template

In a number of cases, partners were also able to provide their input from the events – i.e. images and feedback – while their attendance was ongoing, and this was resulted in LinkedIn posts published in real time.

- Constant communication with all partners was established by email on a regular basis, in order to track and monitor external events participation.
- For those partners presenting the project as speakers, the procedure in place was also envisaged a formal validation of the presentation content through its submission to the Article Validation Committee, which was set up to verify that all external communication observed the security constraints of the project.

### 2.3. List of attended external events

A total of 39 unique international external events were attended by the 7SHIELD partners throughout the project lifetime.

#### Attended events

Table 2-1 lists all attended events, including the relevant details, which are analysed in detail in the points that follow.

Table 2-1 – List of attended Events

Partner attending	Type of Participation	Type of Event	Event Title	Start Date	End Date	Location
SERCO	Speaker	Conference	<a href="#">Phi Week</a>	1-Oct-20	1-Oct-20	Virtual
SERCO	Speaker	Workshop	<a href="#">"Leveraging the EU infrastructures in Europe"</a>	19-Oct-20	19-Oct-20	Virtual
ENG, CS	Speaker	Conference	<a href="#">Nicosia Risk Forum 2020</a>	26-Nov-20	26-Nov-20	Virtual
ENG	Speaker	Conference	2 <sup>nd</sup> Secure Societies "Project to Policy Kick-Off Seminar" (P2PKOS)	22-Mar-21	23-Mar-21	Virtual
SPACEAPPS	Speaker	Workshop	Teleconference on ESA Ground Segment security policy and standards with DG-X, ESIRIN	1-Apr-21	1-Apr-21	Virtual
SERCO	Speaker	Conference	<a href="#">Big Data from Space 2021</a>	18-May-21	20-May-21	Virtual
ENG	Auditor	Conference	<a href="#">Data Week</a>	25-May-21	27-May-21	Virtual
CERTH	Speaker	Workshop	<a href="#">2<sup>nd</sup> International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021)</a>	4-Oct-21	8-Oct-21	Darmstadt, Germany / Virtual
SERCO	Poster	Conference	<a href="#">ESA Φ-Week</a>	11-Oct-21	15-Oct-21	Virtual
STWS	Booth	Exhibition	<a href="https://www.be4ond-expo.gr/">https://www.be4ond-expo.gr/</a>	14-Oct-21	16-Oct-21	Thessaloniki, Greece
SERCO	Booth	Conference	<a href="#">The European Space Forum 2021</a>	8-Nov-21	9-Nov-21	
CS	Booth	Conference	<a href="#">Space Tech Expo   Europe</a>	16-Nov-21	18-Nov-21	Bremen, Germany
CS	Speaker	Conference	<a href="#">Industry Space Days</a>	7-Dec-21	8-Dec-21	Virtual
KEMEA	Auditor	Conference	<a href="#">CERIS Disaster-Resilient Societies (DRS) Event</a>	23-Mar-22	25-Mar-22	Hybrid
SPACEAPPS	Auditor	Workshop	<a href="#">Space 4 Critical Infrastructure - Introduction into the EU-Directive on the resilience of critical entities [WEBINAR]</a>	29-Mar-22	29-Mar-22	Virtual
ENG	Speaker	Workshop	<a href="#">EU-HYBNET 2<sup>nd</sup> Annual Workshop</a>	6-Apr-22	6-Apr-22	Roma, Italy / Virtual
CS	Speaker	Conference	<a href="#">CYSAT PARIS 2022</a>	6-Apr-22	7-Apr-22	Paris, France
STWS		Workshop	<a href="#">CERIS FCT workshop on protection of public spaces</a>	7-Apr-22	7-Apr-22	Brussels, Belgium

CERTH	Speaker	Workshop	<a href="#">2<sup>nd</sup> ECSCI workshop on Critical Infrastructure Protection</a>	27-Apr-22	29-Apr-22	Hybrid
CeRICT	Poster	Workshop	<a href="#">Security Mission Information &amp; Innovation Group (SMI2G) Workshop 2022</a>	16-May-22	17-May-22	Brussels, Belgium
ACCELI	Poster	Conference	<a href="#">DroneWISE final conference (ISFP project)</a>	20-May-22	20-May-22	Šibenik, Croatia
CS, SERCO	Speaker, Booth	Conference	<a href="#">Living Planet Symposium 2022</a>	23-May-22	27-May-22	Bonn, Germany
ENG	Speaker	Conference	<a href="#">13<sup>th</sup> International Conference "days of Corporate Security 2022"</a>	31-May-22	1-Jun-22	Ljubljana
SPACEAPPS	Speaker	Workshop	11 <sup>th</sup> EU-US-Canada Expert Meeting on Critical Infrastructure Resilience	1-Jun-22	2-Jun-22	Paris, France
SERCO, CS, HP	Speaker	Conference	<a href="#">FIC (International CyberSecurity Forum)</a>	7-Jun-22	9-Jun-22	Lille, France
CERTH	Speaker	Conference	<a href="#">CIPRE-EXPO - 2022 Critical Infrastructure Protection and Resilience Europe</a>	14-Jun-22	16-Jun-22	Bucharest, Romania
SPACEAPPS	Speaker	Workshop	<a href="#">EU-HYBNET Innovation and Standardisation Workshop</a>	15-Jun-22	15-Jun-22	The Hague, Netherlands
ENG	Speaker	Conference	<a href="#">37<sup>th</sup> ECASEC EG of Telecom Security Authorities meeting</a>	28-Jun-22	28-Jun-22	Brussels, Belgium hybrid
STWS	Booth, Speaker	Conference	<a href="#">ICONHIC 2022 - 3rd International Conference on Natural Hazards &amp; Infrastructure</a>	5-Jul-22	7-Jul-22	Athens, Greece
STWS	Speaker	Workshop	CERIS INFRA event: "How research supports the directive on the resilience of critical entities?"	12-Jul-22	12-Jul-22	Brussels, Belgium
INOV	Speaker	Conference	<a href="#">ICECET 2022</a>	20 July 2022	22 July 2022	Prague, Czech Republic
RESIL	Speaker	Conference	<a href="#">IEEE International Conference on Cyber Security and Resilience</a>	27 July 2022	29 July 2022	Virtual
SPACEAPPS, CS, DES, DEIMOS	Speaker, Booth	Conference	<a href="#">IAC 2022 Paris</a>	18-Sep-22	22-Sep-22	Paris, France

SATWAYS	Speaker	Conference	<a href="#">3<sup>rd</sup> International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2022)</a>	26-Sep-22	30-Sep-22	Copenhagen, Denmark
SATWAYS	Speaker	Workshop	<a href="#">CERIS FCT/INFRA annual event</a>	27-Sep-22	28-Sep-22	Brussels, Belgium
DES	Booth	Conference	<a href="#">Space Tech Expo Europe 2022</a>	15-Nov-22	17-Nov-22	Bremen, Germany
STWS	Booth	Workshop	<a href="#">International Exhibition BEYOND 2022</a>	29-Sep-22	1-Oct-22	Thessaloniki, Greece
DEIMOS	Booth	Conference	<a href="#">Space Tech Expo Europe 2022</a>	15-Nov-22	17-Nov-22	Bremen, Germany
SATWAYS	Speaker	Workshop	<a href="#">CERIS event on "Innovation Uptake of EU-funded Security Research outcomes"</a>	1-Dec-22	1-Dec-22	Brussels, Belgium





**Partner attendance**

Figure 2-4 lists the number of events attended by partner.

It is worth mentioning that some of the events were attended by more than one partner (i.e. the Nicosia Forum 2020, the Living Planet Symposium 2022, the FIC - International CyberSecurity Forum and IAC 2022 Paris). Although not all 7SHIELD partners managed to ensure events participation, the average attendance on the basis of the total individual attendances (46) and the total number of partners (22) equals 2,09, which is in line with the initial expectation that each partner participates in at least 2 events.

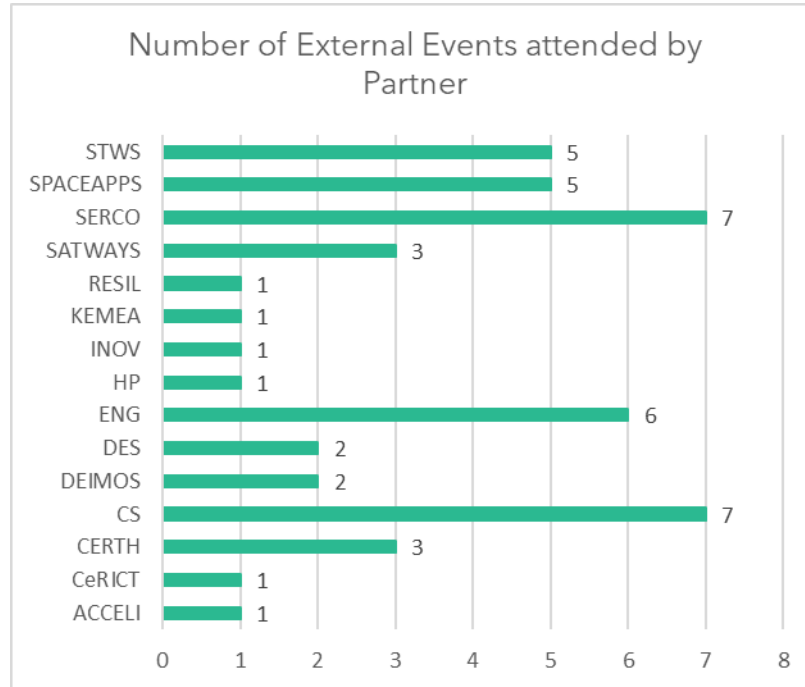


Figure 2-4 – Events – Attendance by Partner

**In-person vs Virtual events**

Figure 2-5 shows the percentage of in-person vs virtual events. Most of the virtual events took place in the first 18 months of the project.

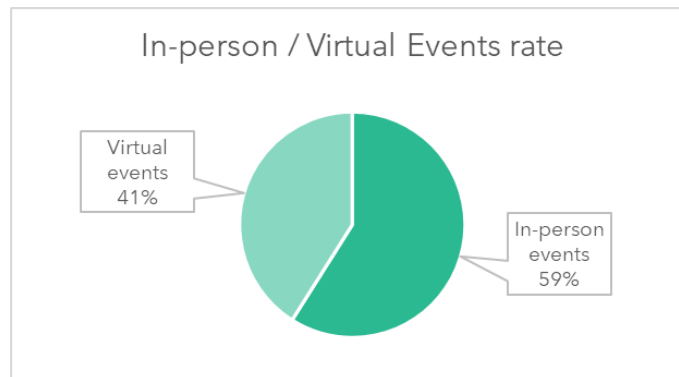


Figure 2-5 – Events – In-person / Virtual rate

**Type of events**

Three typologies of events were identified, namely Workshop, Exhibition and Conference. Figure 2-6 analyses the percentage of event types.

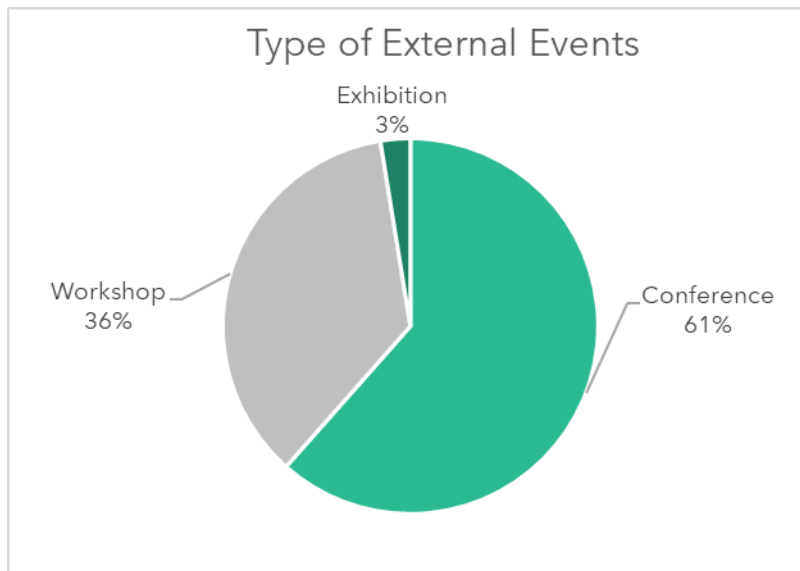


Figure 2-6 – Events – Type of events

### Type of participation

Participation to external events was categorised into 4 types:

1. **Speaker** – the 7SHIELD partner provided an oral presentation of the project, either a general introduction or a more detailed presentation on a specific 7SHIELD topic. Mentions of the project in the context of a more general presentation on the partner’s activities was also taken into account, as they are as well considered effective ways to disseminate awareness of the project.

Table 2-2 – Presentations on specific 7SHIELD topics at external events

Partner	Event	Presentation Title
ENG	2 <sup>nd</sup> Secure Societies “Project to Policy Kick-Off Seminar” (P2PKOS)	7SHIELD Policy Brief
CERTH	<a href="#">2<sup>nd</sup> International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021)</a>	"Severity level assessment from semantically fused video content analysis for physical threat detection in ground segments of space systems"; "A holistic framework to protect Ground Segments of Space Systems against cyber, physical and natural complex threats", on behalf of ENG
SPACEAPPS	<a href="#">EU-HYBNET Innovation and Standardisation Workshop</a>	7SHIELD - EU-Hybnnet - Who needs standards?
STWS	<a href="#">ICONHIC 2022 - 3<sup>rd</sup> International Conference on Natural Hazards &amp; Infrastructure</a>	A Multihazard Risk analysis Platform (presentation including demonstration of specific versions of CIRP and ENGAGE, tools that Satways offer in the 7SHIELD project)
INOV	<a href="#">ICECET 2022</a>	Study on the Application of EfficientDet to Real-Time Classification of Infrared Images from Video Surveillance

RESIL	<a href="#">IEEE International Conference on Cyber Security and Resilience</a>	Modelling and assessing the risk of cascading effects with ResilBlockly
SPACEAPPS	<a href="#">IAC 2022 Paris</a>	Improving ICE Cubes security resilience with 7SHIELD + Booth B1
SATWAYS	<a href="#">3<sup>rd</sup> International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2022)</a>	"Solutions for Protecting the Space Ground Segments: From risk assessment to emergency response". Paper focusing on the CIRP-RAT, ENGAGE PSIM and ERPs components, provided by Satways (the first two) and KEMEA (the last one).

- **Poster** – the 7SHIELD partner contributed to an event through the submission of a poster (printed or digital) or mentioning 7SHIELD. Posters typically also involve a short oral presentation.
- **Booth** – the 7SHIELD partner participated in an event with an exhibition booth, where the project was promoted through direct networking and also through the distribution of promotion material (7SHIELD Brochure and Infoboard) and/or the projection of the project slides.
- **Auditor** – the 7SHIELD partner attended an event with a participant role.

Figure 2-7 below illustrates the split of partners' participation in external events.

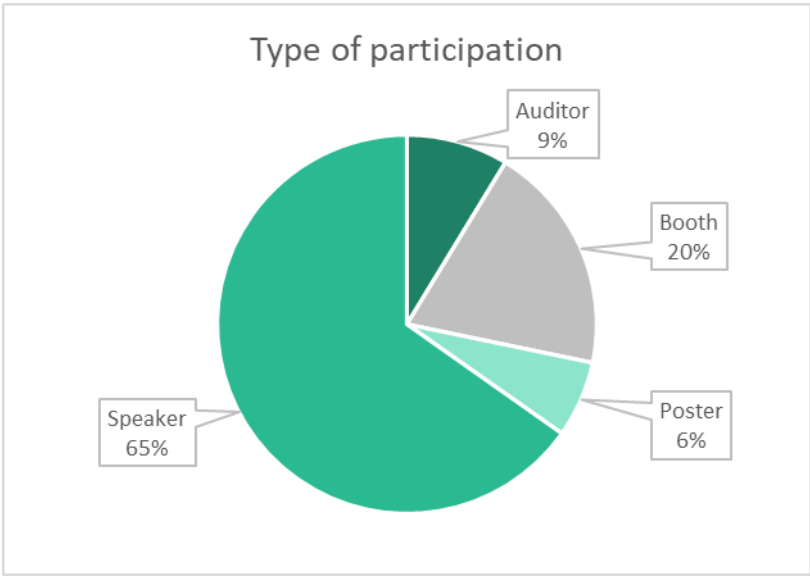


Figure 2-7 – Events - Type of participation

### 3. Collaboration activities

Building networks and collaboration with other projects and stakeholders ensures a proper exchange of information and ideas and enriches the project results and outcomes. The principal aim of this action is to collate information and experiences, to benefit from other projects' outcomes, methodologies, best practices and success stories, to foster networking between coordinating and associated beneficiaries of H2020 and HE, to identify opportunities for further collaboration and to perform profitable and fruitful collaborations.

The objective of the 7SHIELD project partners is, hence, to initiate broad and continuous dialogue with project members and other stakeholders to guide implementation and evolution of security frameworks in Ground Segment domain.

Once the network of contacts is built and members are engaged, 7SHIELD tried to create a strong feeling of community among the different stakeholders around the same objectives to promote exchanges and interactions. For such purpose, there was the need to build the culture of collaboration among all project partners, at first, and co-design the project outcomes.

The diagram below (Figure 3-1) highlights the key capabilities needed for effective co-design. Once mastered, these behaviours can be applied in any setting to promote true partnerships with others.



Figure 3-1 – Collaboration pillars

To reach this objective, several internal workshops and a tailored Info Day were organised in coordination with all contributors within the Consortium with the aim of collecting feedback and improvements from the participants.

#### 3.1. Internal workshops

During the project length, several internal meetings (71 until the end of 2022) were organized in order to collaborate and create a value for the 7SHIELD project.

Here after we mention the main workshops and events that were organized by the project partners with the aim to create a specific outcome.

Table 3-1 – Internal workshops and interviews

<b>Title</b>	<b>Organizer</b>	<b>Participants</b>	<b>Objectives</b>	<b>Outcomes</b>
<b>User requirements workshops</b>	NOA	All the project partners and the invited external stakeholders	Check the collected technical and user requirement via bilateral meetings, confirm or deny their implementation within 7SHIELD project and agree their priority	D2.2: Consolidation of Stakeholder Requirements
<b>Market analysis internal workshop</b>	CS	All the project partners	Identifying existing business models' competitiveness landscape, market size (current and future), market trends, market growth rate, key success factors and key success details related to application of integrated novel technologies aiming to assist the safety and security	D8.7: Market Analysis report v2
<b>Threat taxonomy workshop</b>	RESIL	All the KR owners	Definition of the threat taxonomy that will be used in the project.	Agreed threat taxonomy included into D6.3: Definition of the integration and validation plan and D5.1: The 7SHIELD ontology and data representation model
<b>KR owner interviews</b>	SERCO	All the KR owners	Collection of information on the KRs in order to produce the communication relevant material on their scope, purpose, partners involved (and their email contacts), possible	KR leaflets

			stakeholders, technology or methodology used for their development and future improvements	
<b>Focus groups</b>	Pilot partners (SERCO, NOA, FMI, DEIMOS, SPACEAPPS)	Invited consortium's end-users	Definition of the exact extent of the five pilot areas and the identification of the use cases and user scenarios to be addressed by the project.	D2.1: 7SHIELD Use Cases Design

### 3.2. Tailored Info Day

The 7SHIELD Info Day was organized in Brussels, Belgium on 14 December 2022, under the coordination of SERCO.

The methodology followed by SERCO for the set-up and organisation of the event is presented in Figure 3-2, while Table 3-2 explains in more detail the objectives and activities done at each step reported above.



Figure 3-2 – Event set-up and organization

Table 3-2 – Event organization steps

Steps	Objectives	Outcomes
<b>Sponsor team definition</b>	Establish a list of community members & partners for the event  Coach the speakers to ensure a high quality of discussion	Each person should be selected in relation to the context of the question the event aims at answering, as well as their individual and collective ability to play the role required of them.
<b>Event co-design</b>	The sponsor team is engaged in order to design and define the content of the event and its facilitation.  Usually, 2-6 meetings lasting 2-3 hours (process called “sponsor journey”) is necessary for reaching the design of the event sessions.	Identify the main themes and/or relevant themes and needed material for the event  Build an agenda following the objective and expected results of the event, choosing the way each session will be taken  Model the participants experience in real time during the event also considering the backstage activities.

<b>Communication support</b>	Ensure the visibility of the event	<p>Send invite to the entire community</p> <p>Setting up a registration link to be a participant and attend the event</p> <p>Use of the project member's network to disseminate the messages to the entire ecosystem</p> <p>Publication of the different levels of messages during the period preceding the event, following different formats (mails, LinkedIn, postcards)</p>
<b>Organization of the event</b>	Convening and ecosystem management	<p>Ensure the relevant stakeholders will attend the event</p> <p>Take care of the details for a holistic experience of participants in terms of logistics, physical/virtual or hybrid space, materials to be printed or sent, team of facilitators, organizers and moderators</p>
<b>Event</b>	Ensure the event runs smoothly	<p>Event moderation</p> <p>Stakeholders' interaction</p> <p>Verification of persons present (potential subcontractors, primes, partners)</p> <p>Overall coordination of the event with the sponsor team</p>
<b>Follow-up</b>	<p>Share a survey valuating the workshop, if needed.</p> <p>Ensure efficient Users' feedback</p> <p>Provide event report</p>	<p>Structuring the communication of the event and diffusion on social networks and the website</p> <p>User feedbacks trace</p>

The following sections specify some results and lessons learnt of the various steps of the 7SHIELD Info Day event organization.

### 3.2.1. Sponsor team

The SERCO team identified the people acting as “sponsor team”, meaning the people that identified the objectives, themes and expected results of the Info Day and guided the partners to design the content of the various sessions of the event.

The sponsor team was constituted by people having different backgrounds such as communication, business, technical and project management. They envisaged to be in 2023, 1 year after the event, and listed the results, successes and lessons learned of the past Info Day event. An individual “take a box” exercise was done and each of them answered six (6) simple questions on each side of a box, which they then shared in plenary where all results and comments were collected and discussed.



Figure 3-3 – Individual exercise in order to collect the personal view of the sponsor team on objectives and outcomes of the Info Day

### 3.2.1.1. Objectives

Share how the 7SHIELD framework can protect the Satellite Ground Segments and inform about its flexibility and adaptability in different situation and context.

### 3.2.1.2. Outcomes

Knowledge of the Key Results of the 7SHIELD project; information about the 7SHIELD applicability in the context of the security of Satellite Ground Segments.

### 3.2.1.3. Organization elements

Five (5) organization elements are generally identified during an event organization.



Figure 3-4 – Collaborative discussion during the sponsor team meetings on the five organization

The sponsor team drafted the principal information for each of them and designed the Info Day focusing on the expected participants and the identified themes of the event (as depicted in the image below).



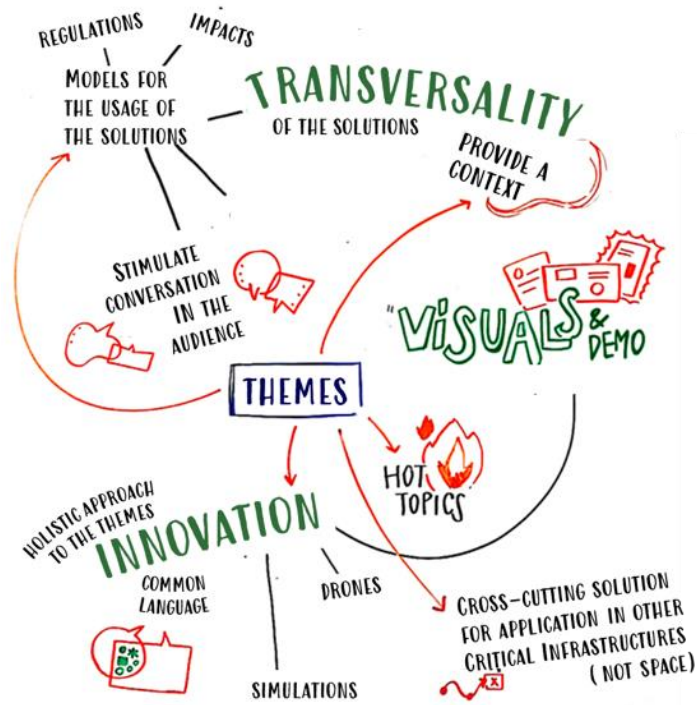


Figure 3-5 – Identified themes of the 7SHIELD Info Day by the sponsor team meeting

The first tangible outcome of the sponsor team and belonging to the “design” element was the high-level agenda which is depicted in Figure 3-6.

# 7SHIELD Info Day Agenda



 This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 883284



Figure 3-6 – 7SHIELD Info Day agenda

The list of targeted actions to carry out in the context of the other elements follows:

## Content

- Involvement of the KR owners, first responders and pilot partners in co-designing the Info Day sessions and for their rehearsal

- Collection of KR owners feedback coming from the internal interviews done for the evaluation of the KR in the Ground Segment domain and production of leaflets summarising the KR description in seven (7) short phrases for each KR.
- Supervision of content creation for the Info Day, providing templates for the partners in order to have a common style for presentations, leaflets, videos etc.
- Production of videos describing how the 7SHIELD framework prevents, detects, mitigates cyber, physical and complex combined cyber-physical attacks.
- Follow up of partners content creation and support, when needed.

### **Convening**

- Planning the date of the event in agreement with the project partners and in order to have the highest probability of external stakeholders' participation (finding a date near another EC event in the same topic);
- Choice of the place where the meeting is held, considering how easy it is to get to, transportation possibilities, parking, etc;

### **Ecosystem management**

- Definition of the IT equipment, the audio-visual equipment, and the wi-fi connections;
- Choice of meals and catering (breaks, lunches);
- Make agreements with the chosen hotel in Brussels for a prebook reservation for all the partners' rooms;
- Maintain the list of participants as well as the number of rooms and dietary requirements for the Serco staff and partners.

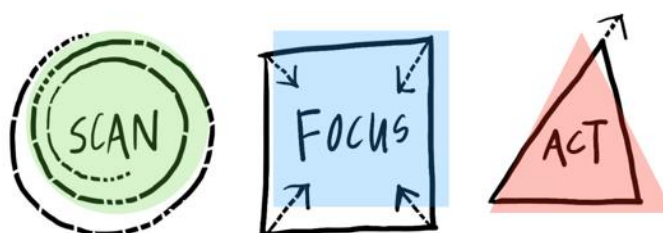
### **Facilitation:**

- Definition of the methodology to follow for each session of the event and identification of facilitation roles: e.g. questionnaires to propose before and during the Info Day to the internal and external stakeholders.

### **3.2.2. Event co-design**

The sponsor team chose to base the design of a collaborative session on MG Taylor's SCAN FOCUS ACT model [1] (Figure 3-7). This was an opportunity to delve into the possibilities offered by the model and to observe its impact on participant engagement.

This model is very natural and distinguishes between different "modes of engagement". In practical terms, it allows a workshop to be sequenced into three (3) phases of (in principle) roughly equal duration, with frequent feedback loops (FEEDBACK).



**SCAN to EXPLORE.** We meet the different stakeholders, discovering their intentions, constraints and objectives, we complete our knowledge of the subject to be dealt with, we look for options, we share information, we create a broad common language, we observe, we conceptualise and we create the conditions necessary to find solutions.

**FOCUS to FOCUS.** This is the stage where we dig. We evaluate and make choices. We reject certain solutions, even the majority of possibilities, and concentrate on a few that we will then evaluate in detail and with rigour. We build solutions that are more concrete and tangible than those conceptualised in the exploration phase. They are tested, iterated and decisions are made.

**ACT for ACT.** Decisions made in the focus phase allow for action to be taken again. We have something to act on. And we plan this action to make these trade-offs viable and resilient. We collectively engage in the implementation of these solutions.

**FEEDBACK for FEEDBACK.** Feedback loops are frequently provoked and regulated. This real-time feedback can take many forms and can come from within the group of participants or from outsiders.

### 3.2.2.1. Partners engagement

The sponsor team used to meet for 1-2 hours each week for a total of fifteen (15) meetings and, with the purpose to involve the partners for the co-design the content of each session, a total of fourteen (14) virtual meetings were organized with all the 7SHIELD partners starting from the beginning of October:

- 2 plenary calls (one at the beginning and one for the final check),
- 4 co-design days,
- 4 calls dedicated to specific sessions of the event and
- 4 rehearsals of the Info Day sessions.

During the co-design days the sponsor team proposed some individual exercises to collect the feedback from all the attendees. The following five (5) topics were proposed and, by using the tool Google Jamboard, the participants were asked to add an anonymous post-it to the whiteboards, then the results were read in plenary, commented and used together to co-create the content of the sessions:

1. **Stakeholders:** Who will participate and why? To what extent are people aware of your problem?
2. **Outcome:** What are the outcomes of the session? How do they fit with the company strategy?
3. **Moods:** What do you want people to THINK and FEEL LIKE at the end of the session?
4. **Goals:** Concretely, what do you hope to hold on your hands when the workshop is finished?
5. **Non-Negotiable:** What are the "givens" and non-negotiable?



Figure 3-8 – Jamboards for the co-design sessions

Several checks on the status of the event organization were done via mail by using a general mailing list generated between partners and a logbook was maintained in order to trace:

- the participants list with their agreed roles during the event,
- point of contact for each session,
- outcomes of each preparatory meeting, the actions taken and solved,
- deadlines and repository for each expected input.

### 3.2.3. Communication support

The Info Day attendance was not expected to include only project members but also invited stakeholders who are experts in any of the project activities.

Invitations and mailing campaigns started three (3) months before the Info Day to maximise participation of key stakeholders and research bodies that are not directly involved in the project or in the external stakeholder consortium.

As part of the communication activities, all the 7SHIELD partners have collected a list of contacts of external stakeholders during the length of the project. This list was built from collaboration gained in different contexts such as other projects, newsletter subscriptions, and participations to events. People belonging to this list received postcards and emails inviting them to the Info Day. The invitations were sent in the form of four (4) tailored communications (one per month starting from beginning of October 2022 + another one only 1 week before the event as a memo).

Moreover, the 7SHIELD LinkedIn account, counting 288 followers, published several posts in the period October-December reminding the upcoming event (Figure 3-9).

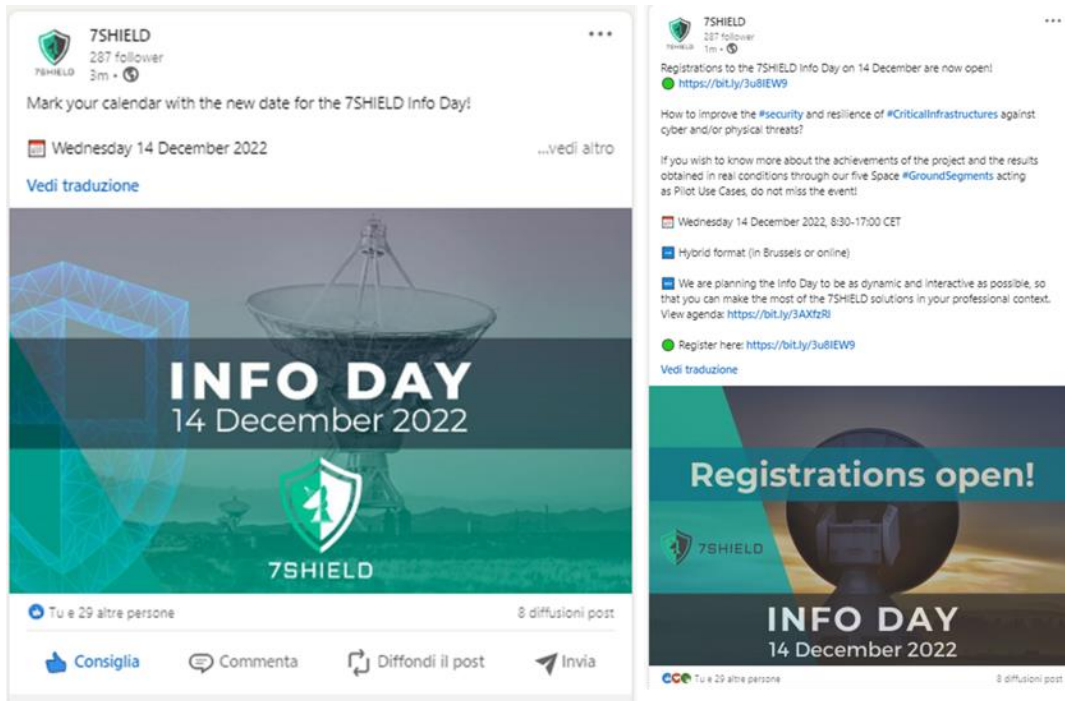


Figure 3-9 –LinkedIn posts for invitation to the Info Day


### 3.2.4. Organization of the event

Before the event, in addition to the organization elements mentioned in 3.2.1.3 section, other important activities were organized. In the following subsections, those were identified for the 7SHIELD Info Day are listed.

#### 3.2.4.1. Theme of the event

For the organization of the event, a main theme was identified, and it was based on the number seven (7), as the seven thematic areas identified for a security framework. For each of them, the 7SHIELD partners provided a definition reported in the Table 3-3.

Table 3-3 – 7 thematic areas definition

Thematic area	Definition
 <p data-bbox="284 1615 440 1675">Situational Awareness</p>	<p data-bbox="523 1487 1385 1585">Situational awareness or situation awareness (SA) is the perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status.</p> <p data-bbox="523 1615 1385 1742">An alternative definition is that situation awareness is adaptive, externally-directed consciousness that has as its products knowledge about a dynamic task environment and directed action within that environment.</p>









 <p>Decision Support Systems</p>	<p>A decision support system (DSS) is an information system that supports business or organizational decision-making activities. Decision support systems serve the management, operations and planning levels of an organization (usually mid and higher management) and help people make decisions about problems that may be rapidly changing and not easily specified in advance—i.e. unstructured and semi-structured decision problems.</p>
 <p>Sensors Technologies</p>	<p>A sensor is a device, module, machine, or subsystem that detects events or changes in its environment and sends the information to other electronics, frequently a computer processor. Sensors are always used with other electronics.</p>
 <p>Semantic Reasoning</p>	<p>Semantic reasoning is the ability of a system to infer new facts from existing data based on inference rules or ontologies. In simple terms, rules add new information to the existing dataset, adding context, knowledge, and valuable insights.</p>
 <p>IoT</p>	<p>The Internet of things (IoT) describes physical objects (or groups of such objects) with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks</p>
 <p>High-level Analytics</p>	<p>High-level analytics can provide an advanced level of data-driven decision making, informing decision makers about different choices with their anticipated impact on specific key performance indicators. In many cases expert-driven techniques are also integrated, offering domain knowledge. They should quickly guide the user to areas where there might be opportunities to improve a process, a state or resilience in general.</p>
 <p>Crisis Management</p>	<p>Crisis management is the process by which an organization deals with a disruptive and unexpected event that threatens to harm the organization or its stakeholders.</p>

Table 3-4 – 7 thematic areas definition

3.2.4.2. Tools

During the preparation of the Info Day, the following tools were implemented. Some of them were physical, some other were virtual (digital) or both. All the tools are listed and described in the Table 3-5:

Table 3-5 – Event tools

<b>Name</b>	<b>Physical/virtual (P/V)</b>	<b>Description</b>
Postcards	P	Printed cards with description, details and registration QR code of the event sent by post for invitation purposes
Badges	P	Light A6 format notebooks with Agenda on back side and participant name on front side
Roll up banner	P	<a href="#">7SHIELD Infoboard</a> displayed in entrance /coffee break room
Printed photos	P	Photos collected from partners, mostly from demo pilots, printed and hanged on walls in entrance /coffee break room
Live questionnaires	V	Live questionnaires using the <a href="#">Mentimeter</a> application used in Sessions 2 and 6.
Posters	P	A3 posters for Info Day Agenda, Objectives and Outcomes hanged in the conference room
Flipchart and post-it	P	2 flipcharts and post-it notes were made available to participants for writing down questions
Chat	V	Live chat on Teams meeting for online participants to ask questions
Thematic area cards	P	Little cards for each 7SHIELD Thematic area (see Theme of the event) used in Session 5: each participant picked a card and approached the part of the conference room where the chosen thematic area was described, and all its KR leaflets were hanged on the wall.
KR cards	P	Laminated A4 cards for extracting the physical elements of 7SHIELD to show their videos and quizzes during Session 6
Brochure	P	<a href="#">7SHIELD Brochure</a> printed for distribution during the Info Day
Leaflets	P/V	A3 leaflets for each Key Results hanged in the room grouped by thematic area; leaflets were also published on the <a href="#">Outcome</a> section of the website and each one of them advertised on the 7SHIELD LinkedIn page in the period 9 November – 12 December 2022.
Live demo of training platform	V	A demo of the Training Platform developed by partner SPACEAPPS
Videos	V	Ad-hoc videos produced by partners for Sessions 3, 5 and 6 according to the specifications provided by the organizers in a sample template.



Presentations	V	PowerPoint presentations by involved partners in session 1, 3, 4 and 7, delivered following specifications provided by the organizers in a sample template.
Logbook and role map	V	Documents to report on Info Day preparation process.
Registration form	V	Online form for participants to register to the Info Day.
Time cards	P	Tool to manage sessions time (cards having different colours and showing minutes remaining to end of presentation's allotted time)
Lunch break slide show	V	PowerPoint slides show including pictures taken during the 7SHIELD project events (pilot demonstration or progress meetings) automatically changing after 20 seconds. Impressed over the images, a text mentioned the expected time the meeting would have restarted. It was used during coffee and lunch breaks.
Music Playlist	V	Music has been used during workshops as a recall to the participants that a session is approaching to its end and it's time to start a new session. The music is initially started softly, and its volume is increased when the time to start the new session is approaching.



Figure 3-10 – Badges, KR and thematic area cards created for the Info Day

### 3.2.4.3. Room setup

The setup of the conference room was planned to change during the day in order to support presentation sessions and interactive sessions. For example, after the lunch break, the room setup was changed in order to provide sufficient space for each working group for sessions 5 and 7 chairs were put in front of the attendees' chairs in order to leave there the cards summarising the "7 reasons why" for each of the thematic area of 7SHIELD. On the walls, the leaflets of the 7SHIELD Key Results were hanged and grouped per thematic area. A thematic symbol in the second map of Figure 3-11 shows the place for each working group.

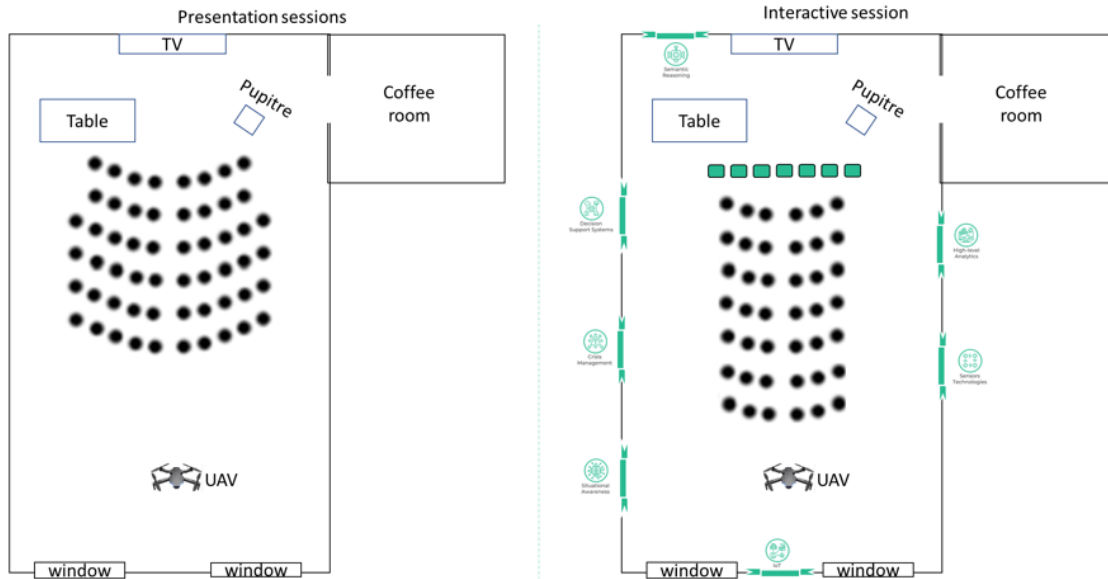


Figure 3-11 – Room setup for presentation sessions and the re-setup of the environment for the interactive session (working groups)

#### 3.2.4.4. Physical presence of a demonstrator

The physical presence of the UAV made by ACCELI (Figure 3-12) was organized in advance because the shipment of the fragile instrument foresaw 1 month of preparation activities and in addition its assembling and disassembling took about 1 hour.

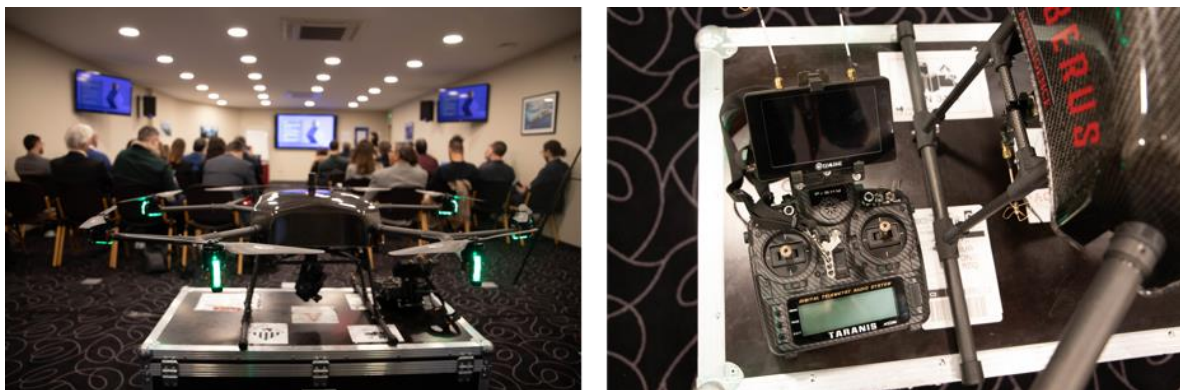


Figure 3-12 – UAV available during the info day

#### 3.2.5. 7SHIELD Info Day Event

104 persons were registered to the 7SHIELD Info Day, including 38 external stakeholders, whose learnt about the event mostly be receiving the invitation by email and word of mouth (Figure 3-13).

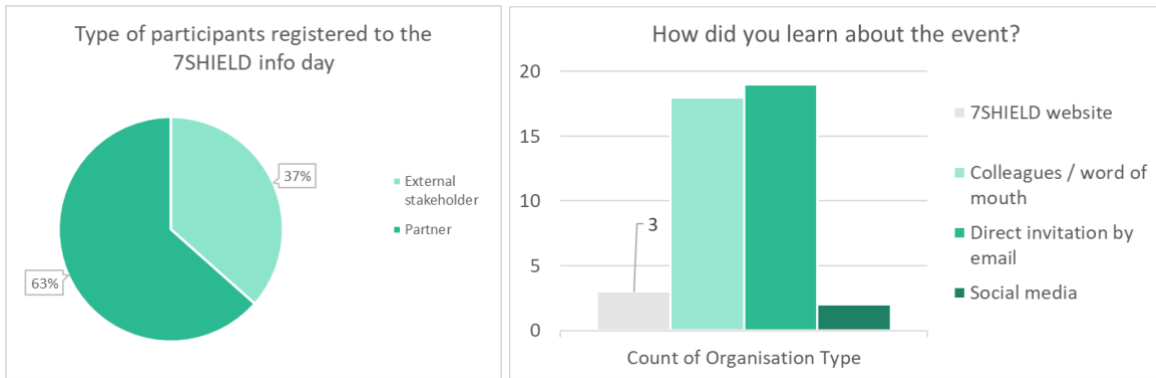


Figure 3-13 – Image of the Info Day registration scores

The organization type of the external stakeholder which were interested to the event were mostly belonging to the public sector or agencies. Only one critical infrastructure owner participated to the event (Figure 3-14).

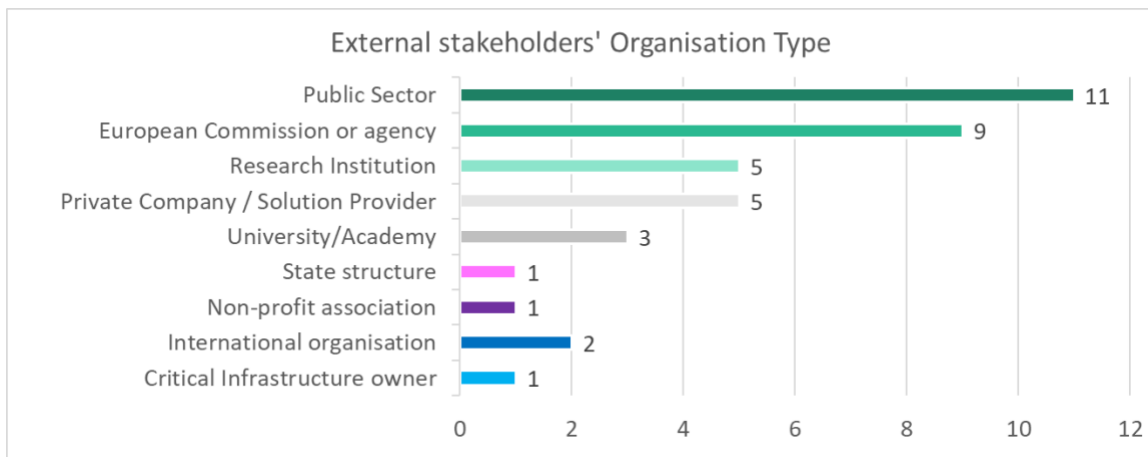


Figure 3-14 – Image of the organization type of external stakeholders participating to the Info Day

80% was the total rate of attendance and 60% of them participated in presence (Figure 3-15): 23 external stakeholders participated and 4 of them were physically present in Brussels.

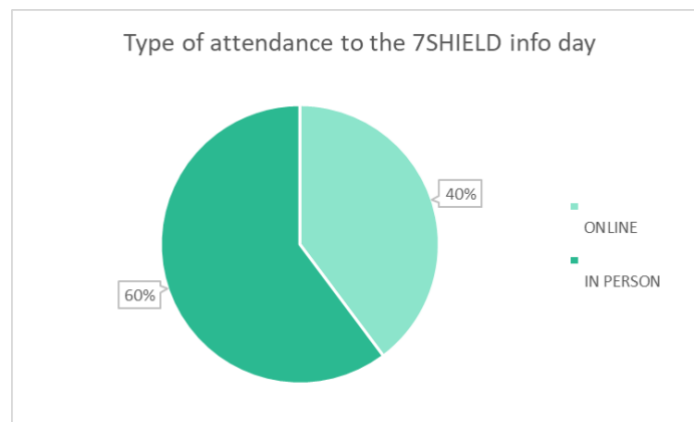


Figure 3-15 – Image of the participation scores

The Info Day aimed at bringing concrete elements, describing the achievements of the project and showing the results obtained in real condition through 7SHIELD five Space Ground Segments, acting as Pilot Use Cases.

Interaction between project partners and external stakeholders was the motto of the event, to assess the value of the 7SHIELD tools in different contexts and its exportability.

During the event, the following ways to promote interaction between participants and keep their engagement high were introduced:

- Live questionnaires
- A physical presence of a UAV
- Presentations in Pecha Kucha mode
- Working groups
- Others, such as videos including music and animations, games, etc...

#### 3.2.5.1. Live questionnaires

A series of seven (7) questions were asked to the participants to answer. This was done by using an online tool, Mentimeter [4], enabling participants to answer questions anonymously by using their phone. Each question was focused on one of the 7SHIELD working areas and provided a multiple choice for its answer, as follows.

1. Have you experienced an external attack or a natural hazard impacting Critical Infrastructures in the last 2 years?

Yes / no

2. Which is, according to your feeling or experience, the highest probable threat / which type of threat worries you most?

Cyber, physical, cyber/physical

3. What type of impact have you registered, or do you expect it to happen?

Multiple choices: stolen user sensible data / data loss / service unavailability / damage to physical assets / phone and computer networks disrupted / paralyze systems / other

4. Considering the most common threat that you faced/may face, when have you alerted / would you alert your end users?

Multiple choices: at the attack detection/ during the attack / immediately after the attack / 1 hour after the attack / 1 day after the attack

5. Considering the most common threat that you faced / may face, how much time was / would be needed for the complete resetting up of the infrastructure and services provided?

less than 1h / 1h - 3h / 3h - 6h / 6h - 1 day / more than 1 day

6. How often do you think the response / disaster recovery and business continuity plan shall be updated considering the evolving technologies becoming "new target" assets subject to "new threats"?

less than 1 year / 1 - 3 years / more than 3 years / never / other

7. What innovation is more interesting for your business?

Multiple choices: Sensors technologies, IoT, Semantic reasoning, High-level analytics, Decision support systems, Crisis management, Situational awareness, other

After each of the questions, the results were interpreted by the moderator and the participants were asked to express their feelings on the results or just comment (Figure 3-16). The results and comments received on the questionnaires are reported in Annex 1 – Results and comments on questionnaires done during the info day.



Figure 3-16 – Questionnaire, live results and comments

3.2.5.2. Presentation in Pecha Kucha mode

The PechaKucha [2] is an alternative presentation style, including 20 slides, each auto-advancing after 20 seconds. It is non-stop and the presenter has 400 seconds to tell a story, with visuals guiding the way. It is sometimes also called a “20×20 presentation”. As a result, the entire presentation always lasts for exactly 6 minutes and 40 seconds (Figure 3-17).





Figure 3-17 – Presentations in Pecha Kucha style

Similar to the short-length focus of an elevator pitch, Pecha Kucha relies upon concision and brevity. By applying a limit on the number of slides, the presenter is forced to streamline their content. It also forces the speaker to prepare and practice, as there is no option to go back or skip ahead. Pecha Kucha is also a very visual presentation style. It is based on few powerful images. Striking visuals enhance any presentation. They captivate the audience in a more immediate way than written words.

### 3.2.5.3. Interactive working groups

Some methods are more efficient in the presence of small groups, which facilitate production of value for the project. These participatory instruments have the objective to stimulate the interaction process and dialogue among stakeholders.

During the 7SHIELD Info Day and, specifically after the lunch break which is usually a time period in which the engagement of the participant is low, the participants were introduced to the interactive session of the workshop which was constituted by three (3) phases:

#### **Phase 1**

The participants were asked to choose a card depicting a thematic area symbol among the seven (7) (see section 3.2.4 for description of the areas). They were guided to the part of the conference room in which there was a thematic area champion (part of the project team) who was there to describe the thematic area and invite the participants to read the various leaflets hanged on the wall, describing the various Key Results developed during the 7SHIELD project and belonging to that thematic area. All the participants choosing a specific thematic area formed a working group and each of the seven working groups were invited to find the reasons why that specific thematic area is important in a security framework.

It is important that such exercise has a time limit and the moderators, walking by the groups, informed them about the time left for the exercise in order to let the group focus on the objective and also provided them with a white poster in which the working groups had to write their results (Figure 3-18).



Figure 3-18 – Phase 1 of the Session in which 7 working groups identified the reasons why the 7SHIELD thematic areas are important for a security framework

At the end of the exercise, the moderator asked to the groups to nominate a representative (different from the thematic area champion) who would present the results of his/her group to all the participants.

### **Phase 2**

The thematic areas were re-described to all the audience and each of the group representative narrated the stories on how they found their results. The moderator, then, asked for further feedback from the other participants (also the remote participants who could not be involved in the previous exercise).

All the results of the working groups, meaning the posters listing the reasons why each thematic area was important for a security framework, are reported in *Annex II – 7 identified thematic areas and the reasons why they are useful in a security framework*. The posters were always visible to the participants during the session (so they continued to think about them in case they were interested and ask to the moderator further details) and seven (7) chairs, in front of the participants, were dedicated to this purpose always available to the attendees. In addition, the list of Key Results belonging to each of the thematic area was useful for pointing the attention to the specific results the 7SHIELD project produced (Figure 3-19).



### **Phase 3**

It is important to share how the seven (7) thematic areas identified for the security framework work together and, for such purpose, a short video explained a practical exercise. Additionally, it was essential to ask feedback also after the video and several questions were collected and reported in *Annex III – Q&A*.

#### **3.2.5.4. Other**

Further elements are useful for promoting interaction among participants and keeping their engagement high.

#### **Videos**

All participants are normally expected to prepare a presentation but, in the era of TikTok and Instagram, short videos, well prepared, including animations, music and using a common structure, voiceover [3] and subtitles are better for engaging people to follow the story and have fun during the event.

#### **Games: Cards for shuffling the execution of videos or live quizzes**

For the sequences of videos, we chose to use some cards and let the participant extract a card which was displaying the name of the video.

In addition, at the end of each video we included a live quiz asking simple questions about the 7SHIELD module or element that was the object of the video just shown. This was done by using an online tool [4] enabling participants to answer questions anonymously by using their phone.

#### **Happy faces**

The easiest way to generate more interest is to create positive emotions of joy, appreciation and gratitude. During the event, the happy faces, no yawning or watching elsewhere (on laptops or mobile phones) are the best way to improve the interaction among people.

All the partners were invited to avoid the use of laptops during the Info Day and in case of any urgent need to use the laptop, they were asked to have a sit in a separate side of the room or in another room of the hotel.

Also, the organizers' and moderators' stay and motion had to be controlled: they should give the impression that things are under control and everything that could influence the positiveness of the day shall be turned into something that brings joy (Figure 3-20).

#### **3.2.6. Follow-up**

After the Info Day, the notes on the results, questions, answers and comments collected during the Info Day were analysed and sent back to the people registered to the event who agreed to receive such information. The content of such information is reported in the Annexes.





Figure 3-20 – Phase 3 of the info day Session in which the identified 7SHIELD thematic areas are shown in action, by using demonstration videos sorted by extraction of cards and followed by quizzes

## 4. Clustering activities

This section documents key clustering activities that took place during the project lifetime, with the objectives to collect information, to feed project evolution's lines, to stimulate exchange of information but also to challenge technologies and ideas with feedback coming from different sources (end users, industrial stakeholders). All in all, this activity aimed to build a community of experts in the security of critical infrastructure, be it physical or cyber, and to feed the vertical and Horizontal network to sustain the continuity of the service at project's end.

The following subsections describe the complementary expertise that was created during key clustering events, highlighting the benefits.

### 4.1. DroneWISE H2020 project

7SHIELD project was invited to the final conference of the H2020 DroneWISE project, which took place in Sibenik, Croatia on Friday May 20th, 2022. Acceligence Ltd., technical partner with strong expertise in drones, attended the event as a representative of the 7SHIELD project consortium.

7SHIELD shares a similar topic with the DroneWISE project, making the exchange of information and sharing of challenges even more interesting. The event emphasized the 7SHIELD solutions relying on the drone technology, highlighting the benefits to the DroneWise partners and end users (Figure 4-1).

DroneWise project actors represent five (5) Member States including Bulgaria, Croatia, Estonia, Germany and Greece, bringing forward a broad European perspective. The main objective was to increase the preparedness of first-responder agencies to better coordinate their efforts, significantly improving the protection of public spaces and coordinated response to a terrorist attack using UAVs. The same objective is shared by 7SHIELD.

The final conference sustained a fruitful panel discussion where the latest trends in C-UAV, experience from practitioners, and need for further research were discussed. The panel was formed by C-UAV practitioners from EU MS authorities. The panel also included questions from the audience to expand the discussion to all realities and perspectives (industry, institutions, laws practitioners, end users...).



Figure 4-1 – 7SHIELD participation to DroneWISE

Various connections were established and are recorded in the below table:

Name	Position
Jana Miriovsky	International Cooperation and Projects Advisor
Antonio Klobucar	Head of the International Cooperation and Projects Department

Jelena Levak	Senior Project Manager
Ines Bolanos Somoano	EC DGHome Bluebook Trainee PhD Researcher of EU Counter-terrorism
Lawrence Gloria	Project Officer (EU Commission DG Home)
Oana Muresan	Relationship Manager & Business Development at Operational Solutions Limited

Table 4-1 – 7SHIELD Connections list

## 4.2. European Cluster for Securing Critical Infrastructure (ECSCI)

7SHIELD project joined as a member ECSCI in January 2021, four months after the project kick-off. 7SHIELD was included in the ECSCI website and mailing list.

The project participated in the international workshops organized by ECSCI on CPS4CIP (Cyber Physical Security for Critical Infrastructures Protection). CPS4CIP responds to different types of market such as finance, energy, health, air transport, communication, gas, and water. This is particularly relevant for 7SHIELD because even if the concept is developed in the Space domain, most of its solution can be re-used in another context.

7SHIELD perfectly fits with the scope of the workshops dealing with Risk Assessment and Management, Integrated (cyber & physical) security, Identification, assessment and mitigation of cyber-physical threats, Automation for detection, prevention and mitigation measures. The project participated in the two annual events in October 2021 and September 2022 presenting its solutions and technologies to security researchers and practitioners from the various critical infrastructure sectors. Workshops were a perfect opportunity to challenge the current security solutions in the light of latest technology developments.

DFSL and Satways Lt, 7SHIELD's partners, successfully submitted a paper for the 2<sup>nd</sup> and 3<sup>rd</sup> annual workshops (respectively in October 2021 and September 2022). The first paper entitled "Towards Improved Detection Systems" focused the physical security with enhanced video surveillance systems for real-time event detection, post-event analysis and extraction of statistical data. The paper presented during the 3<sup>rd</sup> annual workshop, entitled "Solutions for Protecting the Space Ground Segments: From risk assessment to emergency response", emphasizes cyber security tools developed within the framework of 7SHIELD (CIRP-RAT, ENGAGE CSIM and ERP solutions).

## 4.3. EU-HYBNET

The EU-HYBNET project, empowering a Pan-European Network to Counter Hybrid Threats, is a five-year project funded by the European Commission (No. 883054). The project aims at enriching the existing European networks countering hybrid threats and ensuring long-term sustainability. This is achieved by defining the common requirements of European practitioners' and other relevant actors in the field of hybrid threats. Ultimately, this analysis fills knowledge gaps, deals with performance needs, and enhances capabilities or research, innovation and training endeavours concerning hybrid threats.

7SHIELD participated in the Annual Workshop on April 2022. Objectives and main achievements were illustrated by ENGINEERING, focusing on the main innovations in terms of cyber and physical technologies as well as methodological and operational pathways.

The event was a perfect opportunity to emphasize the latest developments in research and innovation activities applied to hybrid threats and to assess them with the 7SHIELD "own" reality (collected from 7SHIELD partners contribution and end users' feedbacks). EU-HYBNET indicates priorities for innovation uptake and industrialization and helps to determine priorities for standardization for empowering the Pan-European network to effectively counter hybrid threats. In this context of standardisation, the

relationship was fruitful with a sustained communication between Dr. Päivi Mattila (LAUREA) and the relevant partners of the 7SHIELD project.

#### 4.4. CERIS

CERIS (Community for European Research and Innovation for Security) aims to facilitate interactions within the security research community and users of research output. Initiated in 2014 by the Commission that established the Community of Users for Safe, Secure and Resilient Societies (CoU), the initiative gathered around 1,500 registered stakeholders (policy makers, end-users, academia, industry and civil society) and regularly held thematic events with the security research community. Now named the Community for European Research and Innovation for Security (CERIS), this platform continues and expands the work of the CoU, considering the forthcoming Horizon Europe developments between 2021-2027.

7SHIELD participated in 3 events: the CERIS FCT: Protection of Public Space (April 2022), the CERIS INFRA 2022 workshop: How research supports the directive on the resilience of critical entities (July 2022) and the CERIS Annual Event 2022: Fighting Crime and Terrorism and Resilient Infrastructure (September 2022).

The audience consisted of law enforcement practitioners, local authorities, infrastructure operators, policy makers, researchers and other experts, making this an excellent opportunity to share technological solutions and market tendency.

The three events gave to Satways R&D Dept, as representatives of 7SHIELD, the opportunity to present the overall approach and the objectives of the 7SHIELD project. Presentations systematically highlighted the following aspects:

- The 7SHIELD tools and solutions that are developed for the direct benefit of the operators and the public agencies
- The adopted standardization framework, which is implemented within the project
- The 7SHIELD platform created for information and data sharing.

Within the framework of the CERIS FCT, critical assets such as public buildings, sports venues, shopping malls, schools, and transportation systems, were indicated as locations very hard to protect while being easily accessible to large numbers of people, making them vulnerable to attack. The sectors covered by the (Critical Entities Resilience) CER Directive do include assets that can be characterized as a public space or soft target. The Space sector has also been identified under the same Directive, as one that do include critical entities making the contribution of 7SHIELD even more valuable.

This aspect has been further developed during the CERIS INFRA 2022's workshop. A panel session "Resilience enhancing research – examples from new sectors covered by the (Critical Entities Resilience) CER Directive" took place, during which Satways Ltd has been invited to contribute to the discussion based on research inputs and findings from the 7SHIELD project. The questions raised by the EC officers in charge for issuing the new directive concluded that 7SHIELD is aligned with the EC's approach for integrating the management of cyber and physical threats using a unified conceptual framework and an interoperable command and control platform.

The 3<sup>rd</sup> event, CERIS Annual Event 2022, gave a special focus on the exploitation and innovation uptake. Indeed, a specific session named "MARKET UPTAKE OF INNOVATION STEMMING FROM RESEARCH PROJECT" allowed Satways Ltd to present the status of the analysis from a 7SHIELD perspective as well as to challenge it with the conclusions shared by other participants. During the panel session, the effective approach of 7SHEILD project was highlighted, also pinpointing how the project benefited from the Horizon Results Booster (HRB). Moreover, the goal of the Panel – the reduction of the distance between research and the market – was tackled by fostering the main

differences between research and commercial products and emphasizing the means to bridge the gap between these two worlds.

#### 4.5. The Security Mission Information and Innovative Group (SMI2G)

SMI2G Event 2022, co-organised by EARTO Security & Defence Research Working Group, the SEREN network, EOS, IMG-S, ECSO and supported by ENLETS, took place physically on 16-17 May 2022 in Brussels. This event gathered European-wide innovators and practitioners who are looking for further consortium partners by presenting game-changing ideas and novel technologies addressing the challenges of Horizon Europe's Civil Security for Society 2022 cluster.

This initiative complements the clustering activities of the 7SHIELD project by creating an ecosystem of experts to define the next topics of innovation in the field of the protection of critical sites. The expertise accumulated by 7SHIELD is an important asset that perfectly fuels these reflections, to build on what has been achieved and provide concrete answers to the question "what's next?", which systematically arises at the end of the projects.

The event was attended by more than 200 individuals with a further 300 listening the keynote speeches and round-table events. Specific sessions like Surveillance and identification, communication systems, resilience, Information Processing & Management and Cyber Security, echo perfectly the 7SHIELD objectives and field of expertise. A poster of the project was presented to representatives of industry, academia, SMEs, and public sector by partner CeRICT srl during the two-day workshop. All presentations from the event have been made available quickly after the event through the SMI2G web page with the contact details of each presenter.

## 5. Conclusions and Future Outlook

---

The clustering and networking efforts supported the participation of people outside the project during the Info Day event of December 14<sup>th</sup>, 2022. 23 people outside the project participated (including 4 physically in Brussels). Relations with the various clusters (H2020 project, EC Initiatives) made possible to precisely know the expectations or challenges faced by the experts and to orient “de facto” the content of the conference, to secure the success of the event. The relationship also allowed the various experts to be aware very early on of the day’s content so that they could assess the relevancy and “block the date”.

On this occasion, extremely interesting discussions were held with some external players, supporting the sustainability of the results obtained:

- The discussion with Mr Frederic Guyomar from EDF (Electricité de France) and representative of the PRAETORIAN project (of which EDF is the Prime Contractor). This project presents many synergies with 7SHIELD, on the objective (“increasing the security and resilience of European CIs against physical and Cyber threat”), but also on the means (“coordinated response system”). The desire to share project’s views and identify key evolution lines was the subject of discussions during the info day. It is obviously necessary to have a formal framework to make such an initiative a reality. The involvement or active sponsorship of EC representatives in these future discussions is mandatory. In addition, the EU-CIP project (<https://www.eucip.eu/>), of which Engineering is the prime contractor, provides an existing contractual framework to supervise the discussion by bringing project representatives around the table. As such, having EDF in the discussion is an asset. EDF is responsible for the French electricity network, therefore a key operator responsible for a highly critical infrastructure for France.
- The contact with Mr Ganesh Sauba from DNV Netherlands was extremely rewarding. DNV Netherlands is an expert in the field of cyber security in the Energy. They combine more than 20 years of cyber security experience with more than 150 years of industry domain and critical infrastructure engineering expertise. Having the relationship establish with such an actor fulfil two objectives of the project:
  - Bringing solution that are relevant for the market, which means that can be integrated or easily plugged to existing operational procedures. In other terms guaranteeing the techno pull rather than techno push, while leveraging the latest technological evolution.
  - Extend the boundaries of the project from the Space community to other domains. 7SHIELD solutions are relevant and applicable to other sector because they are not limited to the Space specificities. Threats have no boundaries, so the response to the threats. DNV could channelled the findings of 7SHEILD fastening the adoption.

More broadly, we can conclude the following based on the clustering and networking activity:

- While the 7SHIELD project had a privileged visibility with other SU-INFRA-01 projects like PRAETORIAN, some relevant exchanges with other H2020 initiatives had taken place like DroneWISE and EU-HYBNET
- These exchanges have been more valuable and numerous towards the end of the project, once the results of the 7SHIELD Use Cases became more and more tangible
- It is essential to keep interactions with the mentioned initiatives and programmes to highlight added values, leverage synergies and avoid duplication of work (CERIS, ECSCI and CPS4CIP, SMI2G)

- The example of implementing the future leveraging the PRAETORIAN and 7SHIELD experience within an existing contractual framework is a motivating approach. It values the achievement of both projects and guarantees a continuous evolution towards improved/consolidated/optimized solutions. Obviously, the discussion should be extended to other relevant projects to benefits from the experience accumulated.
- Due to limited time and resources, few interactions with other interesting stakeholders and programmes took place, notably the ENISA ECASEC expert group and others European regulatory authorities. Some future developments would therefore benefit from collaborating with these initiatives.



## 6. References

---

- [1] Scan-Focus-Act method: <https://www.codesign-it.com/publications/jouer-une-session-en-scan-focus-act-et-loptimiser-en-mesurant-lengagement-des-participants>
- [2] Pecha Kucha Model: "<https://www.pechakucha.com/>"
- [3] Text to speech program for voiceover: <https://voicemaker.in/>
- [4] Live questionnaire and quizzes by using "mentimeter" online tool: <https://www.mentimeter.com/>



## Annex I – Results and comments on questionnaires done during the info day

1. Have you experienced any external attack or a natural hazard impacting Critical Infrastructures in the last 2 years?



Figure 0-1 – Question 1

Comments from HP: Our Organization has a binary role, as on one hand we should protect our infrastructures, and on the other hand support the protection of the critical infrastructures of other organizations. Also, Hellenic Police is responsible for handling cases of hacking of computer systems and theft, destruction or unauthorized dissemination of software, digital data and audiovisual material committed across the country and also supporting other Agencies to investigate relevant cases. Also, our Services are charged with the development of vulnerability assessment and risk management plans, in order to confront these type of attacks and in case of an attack or another serious incident our Services are responsible for the necessary investigation actions. Hellenic Police has contributed to many cases of attacks in critical infrastructures.

2. Which is, according to your feeling or experience, the highest probable threat / which type of threat worries you most?

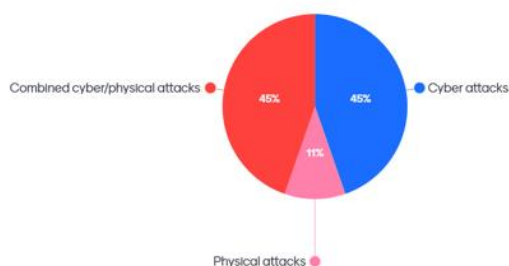


Figure 0-2 – Question 2

Comments from DEIMOS: Physical only or Cyber only are more likely than combined cyber/physical. At Deimos Facilities we see it is more critical to have a Physical attack which also could access critical areas and follow up with a cyber-attack. In this case it is important to include modules for intruders' detection in our facilities in critical areas.

### 3. What type of impact have you registered, or do you expect to happen? (Multiple choice)

Mentimeter

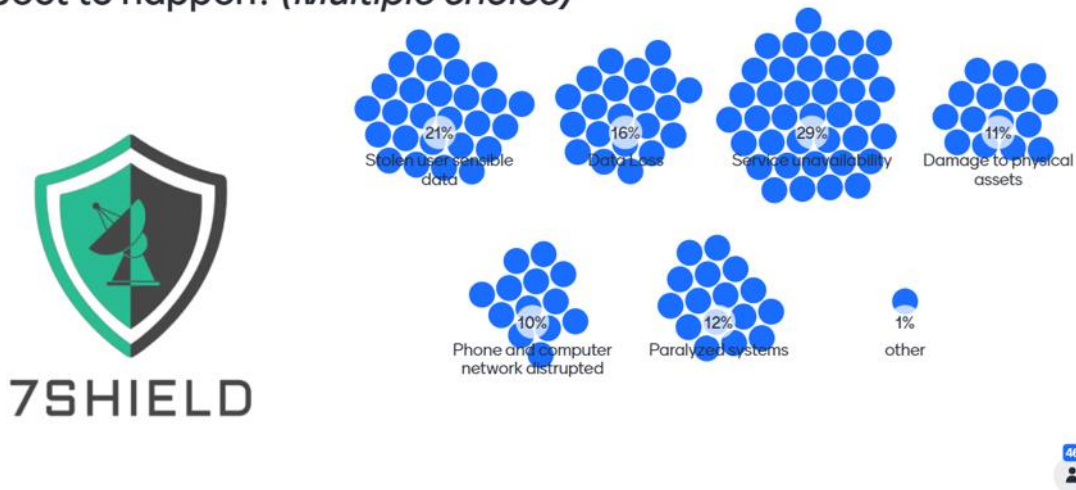


Figure 0-3 – Question 3

Comments from EETT: Among other things, EETT is the competent authority for spectrum management and monitoring. In order to meet its responsibilities regarding radio spectrum monitoring, EETT has created a 24/7 on call service for radio spectrum users of critical infrastructure and services. They can call EETT when they encounter problems that need urgent response, such as interference.

When a harmful interference occurs in wireless systems, users face lack or deterioration of the ability of communication, which results in service unavailability. For the 7SHIELD project we focused on the main communication element of a satellite ground segment which is the frequency used between the satellite and the GS antenna. If an interference occurs on these frequencies, no data (or wrong data) will be received by the GS for processing and dissemination to users. That is why EETT has proposed a detection and identification module as well as a procedure towards neutralizing the interference.

### 4. Considering the most common threat that you faced/may face, when have you alerted / would you alert your end users? (Multiple choice)

Mentimeter

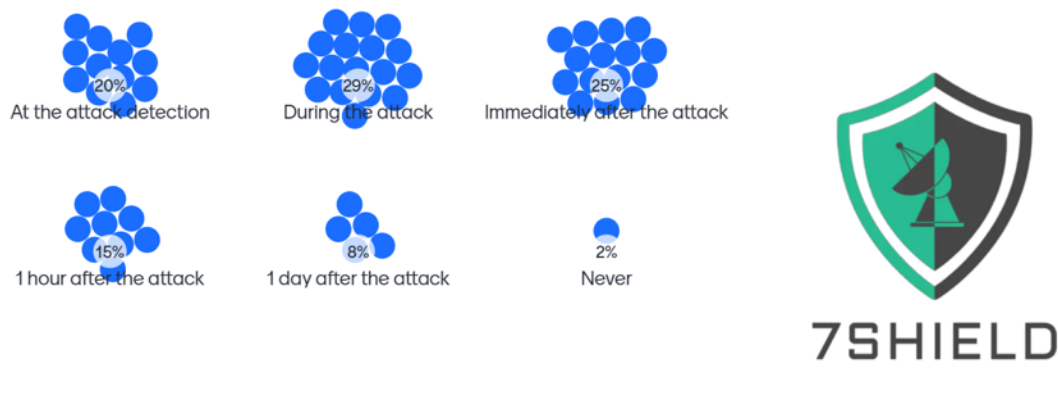


Figure 0-4 – Question 4

Comments from CENTRIC: Centric is a centre of excellence in terrorism, resilience, intelligence and organized crime research. So, we're Research Center at Sheffield Hallam University. Our participation in 7SHIELD was focused on social awareness and message generation. So, this was communication around crisis events, and we looked at a number of best practices and also case studies around these events. You were also mentioning before another aspect just there because we actually found in one of our case studies that we looked at that someone who did communicate before about a storm, a

major weather event, but they didn't communicate with enough sort of urgency. So no one took any sort of preventative action. And then by the time the emergency came around, some of the communication lines had gone down and they weren't able to then get through the people they needed to inform. So, I think also before is important and also to be able to do it with the correct amount of urgency. But I think at all stages we found that communication is important. For example, at the attack detection, it can be it may not be possible for you to communicate, it might only be possible for you to communicate that something is happened, but you may not have enough information at this stage to provide mitigation actions. But as time goes on, the more and more information you want to communicate is what's the potential users should do to mitigate against the attack itself and also what.

We also found that it was important to communicate timescales. So how likely is it that the communication or service is going to come back online? How soon is that going to happen? What are the potential impacts on users? So the most important thing that we found was just that it was important to communicate and not leave people in the dark and they don't know what is happening or how to react and then also, depending on who you're communicating with, so if you're communicating with users, or if you're communicating potentially with citizens or the public and in the area of the ground station installation then this might be a different type of communication.

And the communication requires a dynamic approach anyhow because you might identify an attack and then you might identify what exactly happened and then you might discover slightly later that certain services are still offline. Some services might be able to come back online quickly, some might take longer to come back online. So continual communication about what is going on and also perhaps also in the longer term, you know, what have you done as your organization to potentially prevent this happening again in the future is also another aspect of excellent important to communicate.

### 5. Considering the most common threat that you faced / may face, how much time was / would be needed for the complete resetting of the infrastructure?

Mentimeter

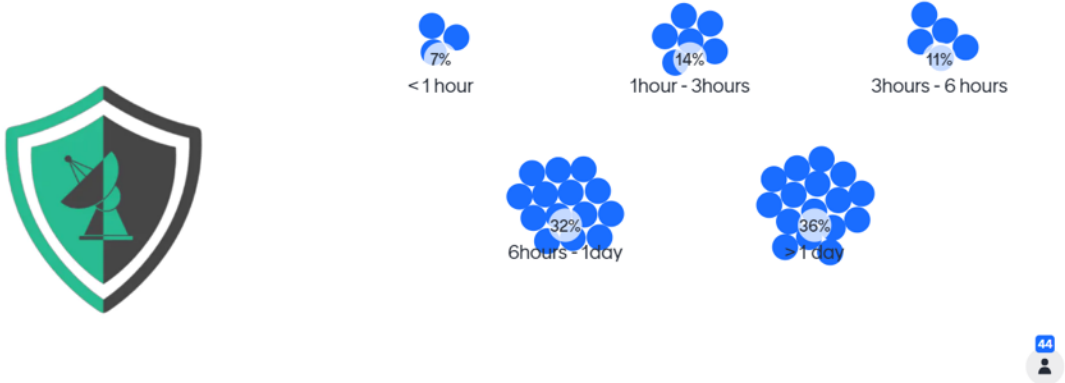


Figure 0-5 – Question 5

Comment from SERCO: Serco is a service company which is managing the operations for the Copernicus Sentinel data access and the ONDA DIAS (Digital Information and Access Service).

We experienced a fire incident in March 2021 disrupting one of the centres of the Cloud service provider in Strasbourg (France) hosting the ONDA and other services.

In terms of service, it collected only two days of unavailability because a disaster recovery plan, involving a complementary centre in GRNET (Greece), was successfully put in place in order to publish the fresh data.

From the user's point of view, the main detrimental impact of the fire was that users' requests of archived user level data were not satisfied for 5 days: the Cloud archive resided in another centre in Roubaix, which was not affected by the fire incident but the interface to it was not available. As a result of the flexibility of the cloud infrastructure, however, it was possible to reinforce the Roubaix data centre by increasing the computing resources. This mitigation solution remained in place for a month, time in which the setup of the infrastructure gradually returned as previously configured. After

this period all the nominal services (also including reporting which were blocked until that period) were recovered.

## 6. How often do you think the business continuity plan shall be updated considering "new targets" and "new threats"? Mentimeter (Multiple choice)

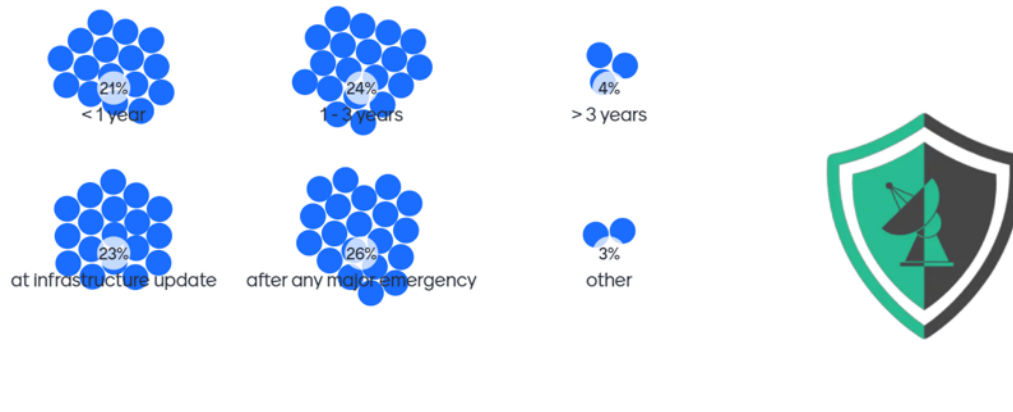


Figure 0-6 – Question 6

Comments from RG: Resilience Guard is a consulting company based in Switzerland with an expertise in business continuity. In our line of business, the frequency of updating the business continuity plan is an important topic of discussion that nearly always comes up when working with clients. The answer depends on the realities of each line of business and the client's specific needs. The wide spread of the answers received reflects in part such different needs, but also some misconceptions that we often see in practice as well.

In general, the business continuity plan corresponds to a snapshot of the client's business, personnel, organization, and infrastructure that is taken at the time of the plan's creation (or its latest revision). Whenever there are significant changes in said parts, one should revise the plan to reflect the new reality. In the case of the ground control stations, for example, if you add or decommission antennas you have correspondingly increased or decreased the resilience in your system; you should update the business continuity plan accordingly. Having faced a major threat, either successfully or unsuccessfully, should similarly trigger at least an internal review of the business continuity plan to identify any potential weaknesses or opportunities for improvement. Barring such issues, one should still plan for periodic reviews and updates of the business continuity plan, simply because organizations and the environment they operate in, naturally change even when working in the "business as usual" mode. Less than a year is too short an interval, more than five years is too long. In most cases an update frequency of three to five years should be adequate.

## 7. What innovation is more interesting for your business? (Multiple choice)

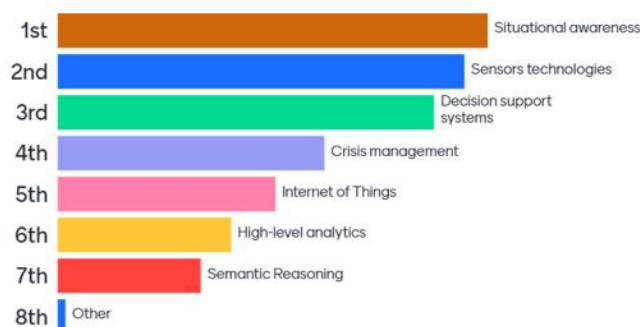


Figure 0-7 – Question 7

Comments from KEMEA: Situational awareness is the missing link between the sensor technology and the decision support systems. In this sense, it's very critical to have a very good overview of what's going on, and of course the importance of the sensors technologies. The decision support system in our view is also critical in order to have an effective and efficient crisis management procedure. But everything is important in the question, but I guess that each category complements the others.

Comments from ENG: All of the thematic areas listed in the choices are part of the 7SHIELD framework, at different scales, of course, and all of them have been contributing to the creation of a situational picture. This situational picture depicts everything that is going on in our infrastructure considering the real time data coming from sensors, considering the Internet of Things devices and the data coming from preparedness and prevention phase.







Such information is relevant in terms of crisis management. So in terms of procedures, in terms of emergency plans, in terms of risk assessment or resilience assessment and the important thing that we have to consider before having an effective evaluation of the current situation, is to put together, not just to looking at the things that are happening real time, but we have to really understand which kind of information we have in terms of how the our infrastructure is resilient, how our infrastructure is prepared against disasters.

So, the situation awareness or the situational picture is the way to provide such kind of unique and coherent view of the situation in our infrastructure.

Comments from DEIMOS: I selected semantic reasoning and that's based on the experience of our pilot. We have several cameras in our building and one of the interesting things of a system like 7SHIELD is the ability to correlate events triggered by the different cameras, in case of a physical attack. So, considering the same person moving in the building and captured by different cameras, if you don't have any ability to correlate this, you'll have multiple alarms.

## Annex II – 7 identified thematic areas and the reasons why they are useful in a security framework

During this session, seven working groups, one for each thematic area, were conducted in order to find some reasons why the thematic areas are useful in a security framework.

Thematic area	Reasons why the thematic area is important in a security framework
 <p>Situational Awareness</p>	<ol style="list-style-type: none"> <li>1. Real time and updated status of the current situation</li> <li>2. Support for decision making through rapid reporting</li> <li>3. Prompt reaction and response</li> <li>4. Better resilience and knowledge of the dynamic environment</li> </ol>
 <p>Decision Support Systems</p>	<ol style="list-style-type: none"> <li>1. Support the management, and mitigation of an incident</li> <li>2. Resilience – increase global resilience of critical infrastructure and entities</li> <li>3. Human activity has an impact on an incident so improving the situational awareness can also reduce the chance of errors</li> </ol>
 <p>Sensors Technologies</p>	<ol style="list-style-type: none"> <li>1. Can provide info to the environment for detection/protection</li> <li>2. Give feedback, trigger events for the users of the system</li> <li>3. They are critical because they are the first POC of the intruder with systems</li> </ol>
 <p>Semantic Reasoning</p>	<ol style="list-style-type: none"> <li>1. Ability to define new rules based on analysis of historical data to issue security alerts and address new security threats</li> <li>2. Correlate multiple events of different origins (cyber/physical/ and even complex hybrid), can also hardcode correlations/queries from domain expertise</li> <li>3. Extract novel security vulnerabilities that were previously unknown</li> </ol>
 <p>IoT</p>	<ol style="list-style-type: none"> <li>1. Support decentralized data collection and fusion of information from remote areas</li> <li>2. Support edge processing and autonomous operations, through the establishment of local smart hubs</li> <li>3. Expandability and upgradability - depending on what the end user needs</li> </ol>
 <p>High-level Analytics</p>	<ol style="list-style-type: none"> <li>1. Risk assessment is the starting point for the operators to understand the vulnerabilities of their systems</li> <li>2. Quantify the possible consequences of an attack</li> <li>3. Severity, i.e how should I respond to an attack (physical/cyber) – need to know severity of the attack</li> <li>4. knowledge is power</li> </ol>



Crisis  
Management

1. Procedures – effective management of the crisis (procedures, processes and IT solutions) - leading to timely management of the crisis, effective communication
2. Autonomous detection and mitigation of threats – ground/aerial based
3. Promptly inform stakeholders using warning message systems / social media. Timely dimensions (detection, mitigation, informed) are particularly important.



## Annex III – Q&A

---

1. **Q. What is the methodology used for the requirements of the 7SHIELD framework definition?**

A (NOA): The requirements were actually defined at the very beginning of the project. We had several activities that took place during the first tasks, which were for the pilot use case, design and user requirements definition. We had basically several rounds of focus groups and interviews with critical infrastructures, security experts and also, with the operators of NOA, in order to discuss past events to map the history of attacks and the frequency, the probability and impact of each type of attack.

We studied, with the help of the Hellenic Police, the situational factors, but exposed our side to natural and man-made threats. The Hellenic Police also did a thorough examination of the premises for physical vulnerabilities, and they provided us with a detailed vulnerability analysis and security recommendations report. This is confidential, but it was used in order to assess the situation and to design a realistic scenario and map the user needs of NOA and we also used the tools provided over the course of the project. And when these tools were made available to the users for the pre-crisis management tools, we did a mapping of all our critical assets and assessment of the threads using the model-based design assessment tool, the cyber risk assessment, physical risk assessment tools or cyber physical threat intelligence. So, we use various methods in order to design a realistic pilot case.

2. **Q: What are the legal consequences of GS service unavailability?**

A (FMI): They are defined in the contract with customers and user. It is user dependent.

3. **Q. How are the instruments protected in the GS?**

A (FMI): In general, if you want to protect them from the human, you need to put them somewhere the human cannot access, or you need to build something around the instruments so they cannot access it. But instead of trying to protect all the instruments, maybe we should have more and more cameras, so the person cannot damage or interrupt only one camera, but there will be many cameras and sensors from different directions and the person will be detected by the systems. And even if one camera goes down, the availability monitoring tool detects if something goes down and creates alert that something is wrong.

4. **Q: Will the 7SHIELD training platform be available to public?**

A (SPACEAPPS): It is planned to be public, but it will require user registration to keep traceability of users and their needs/requests. As there are EU Restricted deliverables in the project, this needs approval from security officer.

5. **Q: Public institutions reporting to national authorities: what level of freedom (or dependency from authorities) do they have to implement new security policies?**

A (NOA): Government authorisation is needed for programs/services mandated by national authorities. For other programs (e.g., Copernicus) there is more freedom to make decisions on security policy, but always within the constraints of contract agreements with program/service stakeholders.

6. **Q. We are working in the era of the social networks and so on. What about the fake news? Is this something that you focus on as well when you have to communicate with the end user, that they heard a lot of messages, and you have to manage the fake news – maybe this was not something we had to deal with in the past.**

A (CENTRIC): It wasn't something which we looked at in the project but communicating early about the attack is that also potentially helps prevent and stop fake news or misinformation spreading.

7. **Q. How to discover relevant information concerning potential new types of attack in the social media or in the web that might be surface web, deep web, dark web? And how to do that?**

A (ENG): Using the technologies in the prevention and the preparedness phase, we have investigated about the possible implementation of the cyber physical threat, intelligence, cyber, physical threat. Intelligence is a way to further investigate, to analyse the available



data source, mainly based on internet like Twitter or Facebook or whatever is evident or not evident, searching for evidence that something might possible and might be happened in our infrastructure and how to correlate such information with the evidence that we are collecting from the sensors for instance. So this is something that in some case might help the process to further investigate and identify potential threats that it's not yet occurred, something that might happens in the next days, but the operators might be informed that it might happen and they are prepared.

8. **Q. How do you manage the human factor during the crisis management?**

A (KEMEA): Third element (in additional to processes & tech). Tech facilitates human reaction, interaction, to allow effective mitigation. Response plans are created by humans to deliver a coordinated response.

A (SERCO): We suggested, as pilot, to try to automatize the response to attacks as much as possible.

9. **Q. How could the GS security be improved by using the IoT?**

A (ACCELL): IoT support decentralised data collection and fusion of information from remote areas and autonomous operations, through the establishment of local smart hubs. Considered the special characteristics of a typical GS – large scale areas, away from main (city) infrastructure – they cannot be supported by typical communications links / networks, may not be reachable by human/machines due to the environment or the morphology of the area. We propose to enhance the operation of the typical IoT operations by using remote smart hubs and to make them to work and operate independently and autonomously. We can receive information with backups from other hubs if one goes down/is compromised. Attackers also have good knowledge/technology therefore we need systems that can adapt quickly to new threats.

10. **Q. There are links between climate change and cyber security risks that may not necessarily be associated with one another, for example malicious attacks timed for when extreme weather events are forecast, where the damage may be greater and response capacities more stretched, or physical damage to infrastructure that can present opportunities for data breaches (for instance power outage caused by extreme weather).**

**How could 7SHIELD strengthen the resilience of the infrastructure against malicious attacks while reducing disruption brought on by climate change and cyber security breaches?**

A (CERICT). We provide an holistic framework with the combination of cyber and physical correlators: we combine different kinds of alerts of different nature, therefore we provide the potential to face this kind of issue because for example, if we detect anomalies and if these anomalies are connected to an intrusion or just something related to climate or error in the measurement, for example, we will detect it and now we will be able to correlate these with the loss of data, for example.

So I think that the 7SHIELD framework could, actually, face this kind of complex combination of threats. Maybe not with the actual scenarios we contemplate, but with maybe more kind of detectors or more sensors or more probes.

11. **Q. How resilient is 7SHIELD to malicious attacks combined with the extreme weather events (for example major storm event). Have you looked into it the scenarios?**

A (ENG). In terms of resilience, it's quite clear which are the benefits 7SHIELD is providing for strengthening the resilience of the infrastructure, either in terms of preventing tools (considering the analysis of the risk, cyber physical, natural hazard, considering also the analysis of the interdependencies and cascading effects, and the analysis of the infrastructure per se), in terms of assets and systems and existing applications (with the model based design application), but also in terms of how to mitigate the disruption in terms of crisis management and we have said which kind of solution we can provide in terms of crisis management procedures and solutions which goals is to reduce the impact of the cyber-physical threats against the Critical infrastructure.

So this is something that, independently of the climate changes that probably here is something that have to be considered as very long term threat, for sure, in terms of physical threats, the extreme weather and cyber security threats, either in terms of properness and response, 7SHIELD can provide a consistent and effective solution.

12. **Q: How much time is needed to configure the UAV by the end-users?**

A (ACCELL): 7SHIELD UAV is a prototype, so the expert needs around 20 min to set up. However, in manufacturing production, a non-expert user would set it up in a couple of minutes. The only thing that he/she should do is to assembly the wings.

13. **Q: Why is FRSS classified as post-crisis tool and not as a crisis tool?**

A (INOV and ENG): The FRSS is a tool for responding to the crisis. The reason for this misunderstanding is that the limits between the crisis management phases sometimes are not so distinguishable. Although, this tool can be also used as a tool during the crisis to identify potential threats by FR teams, however, in the 7SHIELD pilot use case scenarios, this tool was exploited as a response and mitigation action tool.

14. **Q: Is the Radio-Frequency Interference so common a situation as it was demonstrated in the pilots (NOA and FMI)?**

A (EETT): It is common for satellite ground segment installations not to be located too close to densely populated areas, so most of the time there are not as many operating systems that could inadvertently create interference in the area. This is why more isolated places are chosen so that the satellite antenna is as free from any interference as possible. In the case of areas closer to cities, interference can be more likely. For example, there can be interference caused by problems with the management or maintenance of installations so that some transmitters may deviate from the frequency they were allowed to operate on or transmit in different directions, so that they target the GS receiver antenna and cause interference. This interference is unintended, but there may be some cases of intentional interference because someone wants to disrupt the service provided by the ground segment operators. You cannot predict when a malicious user will attempt to create interference resulting in disruption of the service.

15. **Which is the main role of DCEP in 7SHIELD?**

- To autonomously inspect the areas around a space critical infrastructure
- To confirm the presence of an intruder after an alert
- To detect and follow an intruder

16. **Which are the main limitations that 7SHIELD UAV experienced?**

Power consumption

17. **What is the main output of the face detection and recognition (FDR) module?**

It produces alerts when unauthorized persons try to access a secure area

18. **Which are the differences between VOD, ODE and AR?**

VOD and ODE can detect persons in a sequence of video frames while the AR can recognize only their activities

19. **What is the main component of the MMAS?**

A thermal camera

20. **What type of parameters should be taken into account, in order to correlate physical events?**

- Type of the event,
- Location of the event,
- Type of the detector

21. **What are the main features of CIRP-RAT?**

- It is a risk assessment tool analysing physical threats, vulnerabilities and impacts

- It is a web-based tool, built upon a microservices architecture
- It supports the CI owners and operators to enhance their preparedness against potential incidents

22. Is the detection of intruding drone done in all 360 degrees?

Yes

23. What tasks are performed by Flying Hunter?

- It flies to intruding drone
- It catches the intruding drone
- It brings the intruding drone and drops it at a predesignated location
- Forensic analysis of the intruding drone is possible

24. Which technology is used for detection in Laser Fence Sensor?

LIDAR Technology

25. Is the images and track of the intruder stored in the computer for future analysis?

Yes

26. What could be the result of an interference in the frequency that is used by the antenna for reception of the satellite signal?

- Total loss of the satellite data reception
- Degradation of the reception
- Replacement of the received data stream with a false one

27. What is the function of the RFID module in the 7SHIELD platform?

It monitors the reception parameters at the ground segment antenna, detects anomalies and produces alerts



*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883284*