



## D8.3 Project Website

Work Package:	WP8	
Lead partner:	CS GROUP (CS)	
Author(s):	Xavier Pothrat (CS)	
Due date:	30 November 2020	
Version number:	1.0	Status: Final
Dissemination level:	Public	

Project Number:	883284	Project Acronym:	7SHIELD
Project Title:	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats		
Start date:	September 1 <sup>st</sup> , 2020		
Duration:	24 months		
Call identifier:	H2020-SU-INFRA-2019		
Topic:	SU-INFRA01-2018-2019-2020 Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe		
Instrument:	IA		

## Revision History

Revision	Date	Who	Description
0.1	25/11/2020	CS	First release of the draft version
0.2	27/11/2020	CS	Second release of the draft version
0.3	30/11/2020	CS	Third release of the draft version
1.0	30/11/2020	ENG	Final version

## Quality Control

Role	Date	Who	Approved/Comment
1 <sup>st</sup> reviewer	30/11/2020	RG	Approved
2 <sup>nd</sup> reviewer	26/11/2020	KEMEA	Approved
Technical manager	27/11/2020	CERTH	Approved

## Related deliverables

ID	Title	Lead partner	Dissemination level
D8.2	<i>Corporate identity and logo</i>	CS	<i>Public</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

---

7SHIELD website ([www.7SHIELD.eu](http://www.7SHIELD.eu)) is a central tool for the dissemination, communication and networking activities of the project. This document aims to describe the key points of the design, content, maintenance, updating and use strategy of the website.

The document presents the structure of the site and explains how the content is organised across the different pages and sections. It is illustrated by a series of screenshots of the website.



# Table of Contents

Executive Summary .....	4
1. Introduction .....	8
2. Website structure.....	9
3. Website content.....	10
3.1. Common header .....	10
3.2. Common footer.....	10
3.3. Home page .....	11
3.3.1. Project section .....	11
3.3.2. Consortium members section.....	11
3.3.3. 7SHIELD framework section .....	12
3.3.4. Pilot Use Cases Section .....	13
3.3.5. News & Events section .....	14
3.3.6. Contact section.....	14
3.4. Project page.....	15
3.4.1. Concept page.....	16
3.4.2. Outcome page.....	17
3.5. Pilots Page .....	18
3.5.1. Pilot Use Case pages .....	19
3.6. Report & publications page .....	21
3.7. Media page.....	23
3.8. Consortium page .....	24
3.8.1. Partner pages.....	25
3.9. News & Events page .....	26
3.9.1. Newsletters page.....	27
3.9.2. Events page .....	28
3.9.3. Links page.....	29
3.10. Contact page.....	30
4. Website strategy.....	31

## List of figures

Figure 3-1 - 7SHIELD common header.....	10
Figure 3-2 - 7SHIELD common footer .....	10
Figure 3-3 – 7SHIELD Home page – Project section .....	11
Figure 3-4 – 7SHIELD Home page – Consortium members section .....	11
Figure 3-5 – 7SHIELD Home page – 7SHIELD framework section .....	12
Figure 3-6 – 7SHIELD Home page – Pilot Use Cases section .....	13
Figure 3-7 – 7SHIELD Home page – News & events section .....	14
Figure 3-8 -7SHIELD Home page – Contact section .....	14
Figure 3-9 - 7SHIELD Project page.....	15
Figure 3-10 - 7SHIELD Concept page (abstract) .....	16
Figure 3-11 - 7SHIELD Outcome page (abstract) .....	17
Figure 3-12 - 7SHIELD Pilots page .....	18
Figure 3-13 – SERCO’s Pilot Use Case page (abstract) .....	20
Figure 3-14 - 7SHIELD Reports & publications page .....	22
Figure 3-15 - 7SHIELD Media page.....	23
Figure 3-16 - 7SHIELD Consortium page .....	24
Figure 3-17 – CeRICT’s individual page .....	25
Figure 3-18 - 7SHIELD News & Events page.....	26
Figure 3-19 - 7SHIELD Newsletters page.....	27
Figure 3-20 - 7SHIELD Events page (abstract) .....	28
Figure 3-21 - 7SHIELD Links page (abstract) .....	29
Figure 3-22 - 7SHIELD Contact page .....	30
Figure 4-1 - Analytic report on 7SHIELD website audience .....	34

## List of Tables

4-1 - Main target audiences of the 7SHIELD website.....	34
4-2 - 7SHIELD website KPIs .....	34

## Definitions and acronyms

CA	Consortium Agreement
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
C/P	Cyber/Physical
DoA	Description of Action
EC	European Commission
EU	European Union
GA	Grant Agreement
GS	Ground Segment
GSSS	Ground Segments of Space Systems
PC	Project Coordinator
SC	Scientific Coordinator
TM	Technical Manager
WP	Work Package

## 1. Introduction

---

7SHIELD website ([www.7SHIELD.eu](http://www.7SHIELD.eu)) is central for communication activities toward the different targeted audiences and plays a role in the dissemination of 7SHIELD results. The website main objectives are to inform the public on the project status and its evolution, to relay the newsletters and give insight on 7SHIELD results and publications.

7SHIELD website will enable in particular:

- to provide an overview of the project, its objectives, its main milestones and the profiles of consortium members;
- to stay up to date on 7SHIELD progress throughout the project, with the diffusion of newsletters, brochures, info boards and a video;
- to give access to all public deliverables produced during the project;
- to foster the involvement of the various stakeholders and support the organisation of the different events with a calendar, a contact form and information about all the coming events organised by the consortium or related to its activities;
- to create awareness for the project and collect feedback from stakeholders;
- to provide access to the dissemination material and reference to the open access publications produced within 7SHIELD project;
- to facilitate the interaction between partners and interested parties.

## 2. Website structure

---

7SHIELD website is available at [www.7SHIELD.eu](http://www.7SHIELD.eu) and is developed following a responsive web design. It means that the website dynamically changes its appearance depending on the screen size and orientation of the device being used to view it. The domain name has been chosen to be easily found via search engines and the web site is accessible to anyone, without restriction.

Overall graphic design of the Website is aligned with 7SHIELD corporate identity detailed in **D8.2 Corporate identity and logo deliverable**. The interfaces and contents are in English, to be understood by the largest audience and by all consortium partners.

The Website is designed to address the identified target groups in the most effective way, and is the easiest way to ensure high visibility of the project for the EU officials as well as target audiences, stakeholders and the general public.

7SHIELD website contains 8 main pages and 10 sub-pages:

- HOME
- PROJECT
  - CONCEPT
  - OUTCOME
- PILOTS
  - CYBER/PHYSICAL ATTACK IN DEIMOS GROUND SEGMENT - SPAIN
  - CYBER/PHYSICAL ATTACK IN NOA GROUND SEGMENT – ATHENS, GREECE
  - CYBER ATTACK ON ONDA DIAS PLATFORM
  - THREAT DETECTION & MITIGATION ON THE ICE CUBES SERVICE
  - PHYSICAL ATTACK IN ARTIC SPACE CENTER – SODANKYLA, FINLAND
- REPORTS & PUBLICATIONS
- MEDIA
- CONSORTIUM
- NEWS & EVENTS
  - NEWLETTERS
  - EVENTS
  - LINKS
- CONTACT

## 3. Website content

---

### 3.1. Common header

All 7SHIELD website pages have a common header composed of 7SHIELD logo to the left, and the drop-down menu to the right.



Figure 3-1 - 7SHIELD common header

### 3.2. Common footer

All 7SHIELD website pages have a common footer composed with 7SHIELD logo, the European flag, a reference to European Commission financial support to the project and a link to 7SHIELD LinkedIn page (<https://www.linkedin.com/company/7shield>).



Figure 3-2 - 7SHIELD common footer

### 3.3. Home page

The HOME page (<https://www.7shield.eu/>) provides an overview of the project and includes 6 sections linked to other pages of the website.

#### 3.3.1. Project section

The first section displays a short title, the official title of the project and a button that redirect to PROJECT page (<https://www.7shield.eu/project/>).

This section has been especially designed to give a strong visual identity to the project. The background displays the same image used in 7SHIELD presentation template and colours follow 7SHIELD graphic charter. Both are described in in **D8.2 Corporate identity and logo deliverable**.



Figure 3-3 – 7SHIELD Home page – Project section

#### 3.3.2. Consortium members section

The second section introduces the partners. Their logos are displayed in a carousel and each one redirects to the CONSORTIUM page (<https://www.7shield.eu/consortium/>).

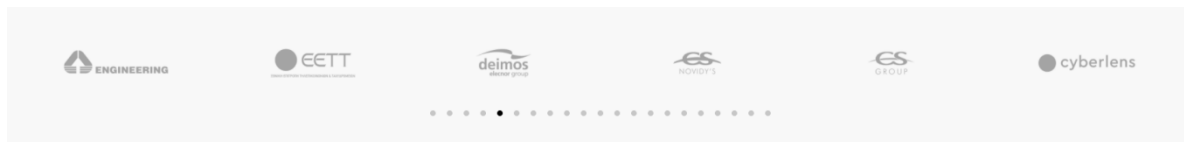


Figure 3-4 – 7SHIELD Home page – Consortium members section

### 3.3.3. 7SHIELD framework section

The third section introduces 7SHIELD framework and its technology bricks (or “key results” as in the proposal). The “key results” are gathered in 4 categories corresponding to the 4 steps of crisis management. Each key result redirects to the OUTCOME page (<https://www.7shield.eu/outcome/>).

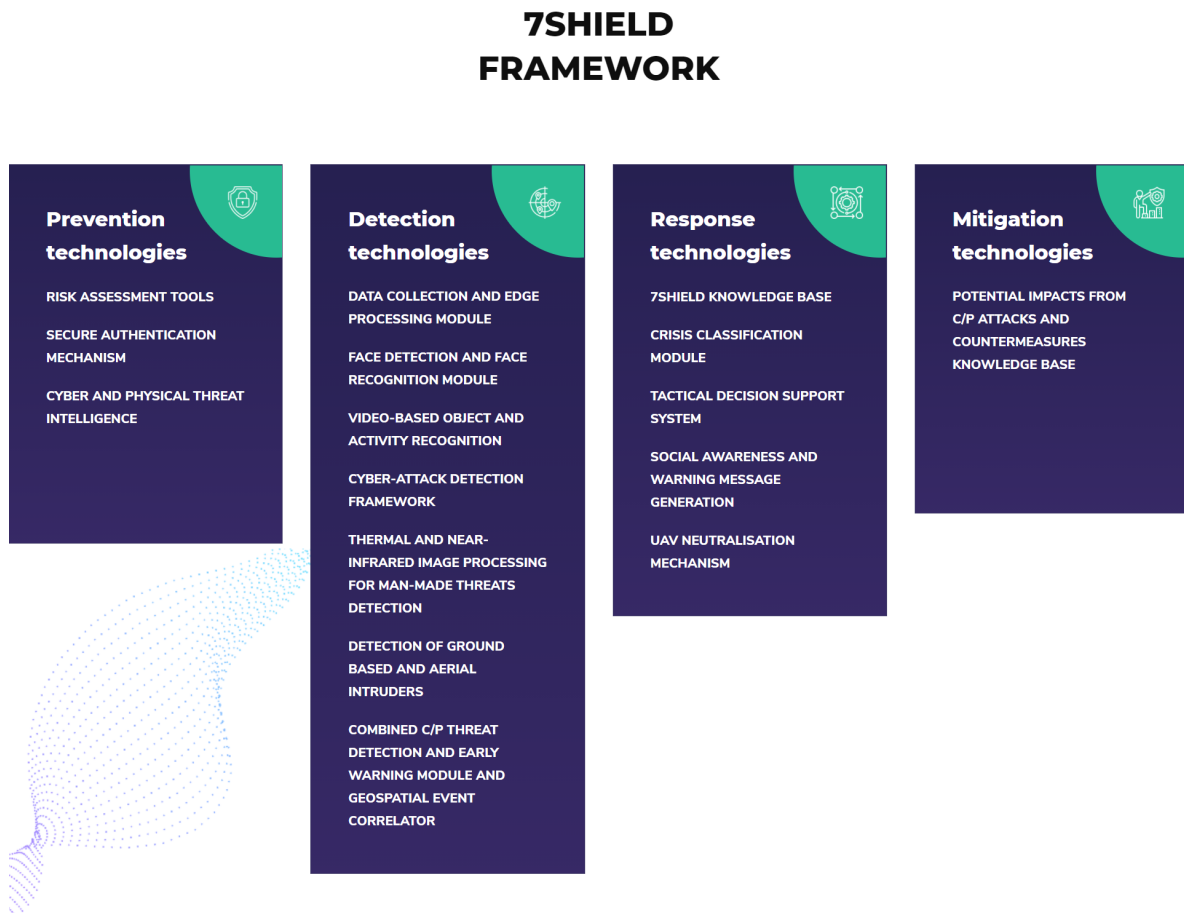


Figure 3-5 – 7SHIELD Home page – 7SHIELD framework section



### 3.3.4. Pilot Use Cases Section

The fourth section introduces the Pilot Use Cases that will be carried during the project. It is composed of 5 snippets, 1 for each Pilot Use Case. Each snippet redirect to the page dedicated to its related Pilot Use Case. At the top of the section, a “VIEW ALL PILOTS” link redirects to the PILOTS page (<https://www.7shield.eu/our-pilots/>).

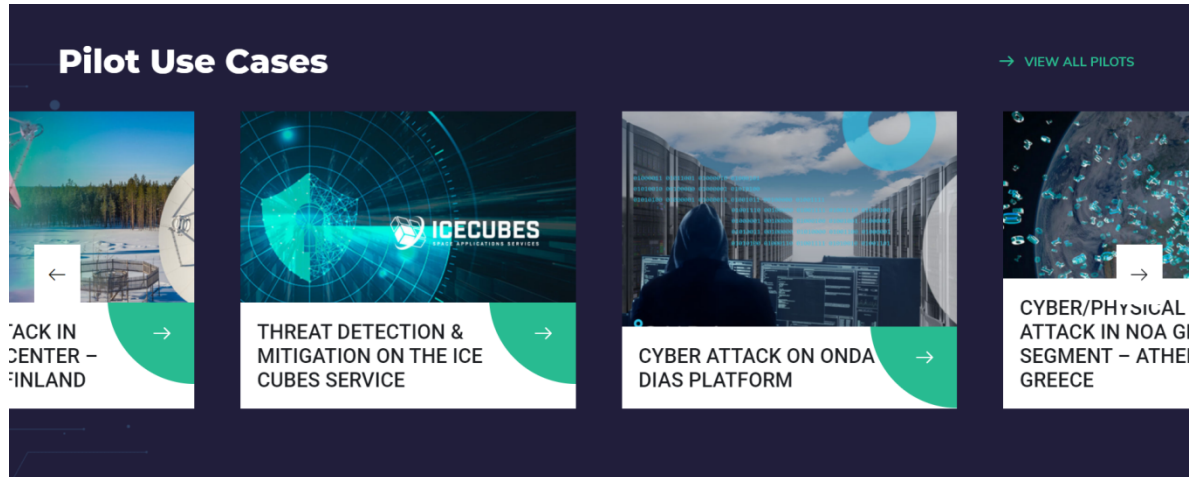


Figure 3-6 – 7SHIELD Home page – Pilot Use Cases section

### 3.3.5. News & Events section

The fifth section gives an overview of 7SHIELD's last news through articles snippets that redirected to the related articles. An "ALL NEWS" button redirects to "NEWS & EVENTS" page (<https://www.7shield.eu/blog/>).

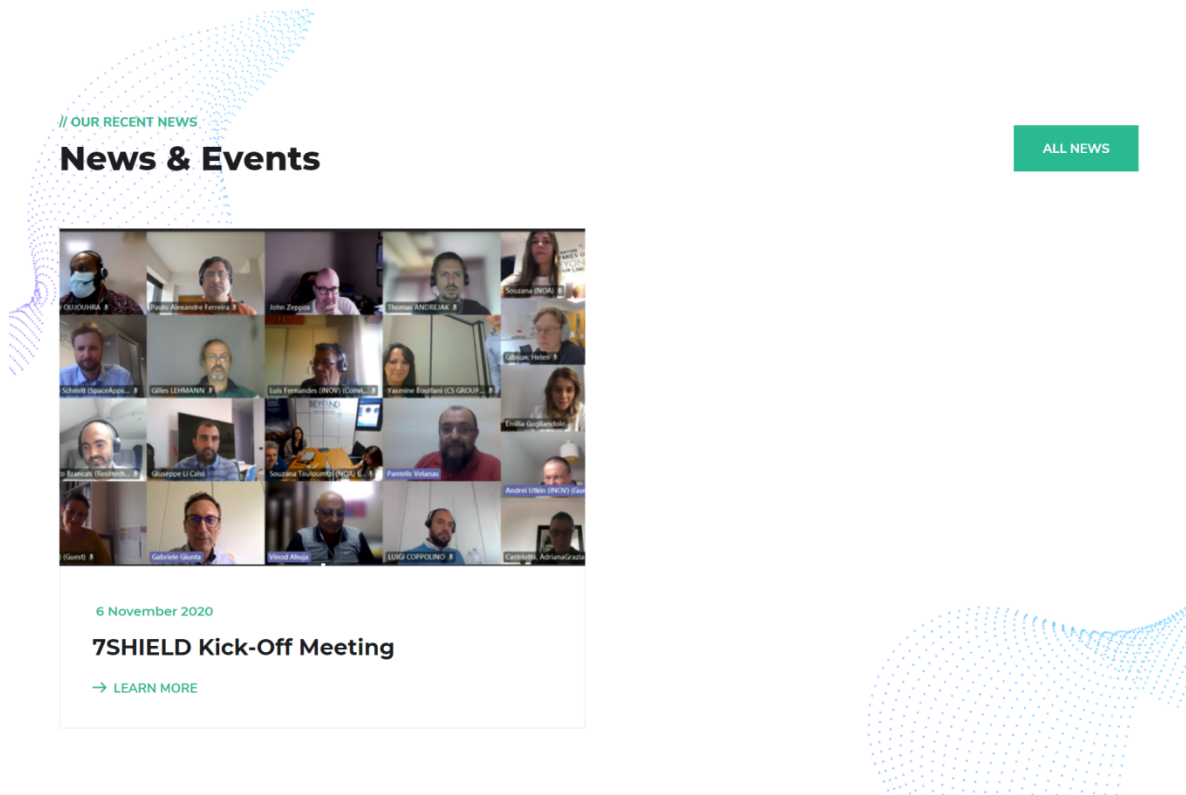


Figure 3-7 – 7SHIELD Home page – News & events section

### 3.3.6. Contact section

The sixth and last section displays a "CONTACT US" button that redirects to the "Contact" page (<https://www.7shield.eu/contact/>).

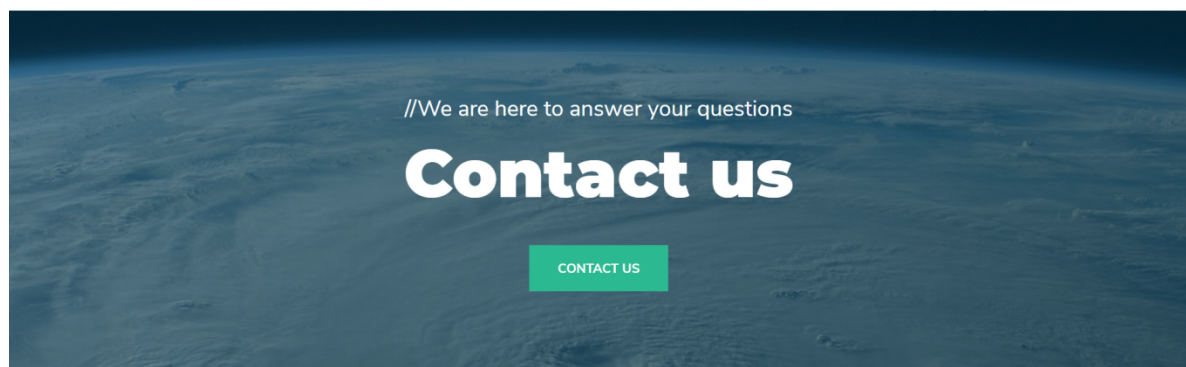


Figure 3-8 -7SHIELD Home page – Contact section

### 3.4. Project page

The PROJECT page (<https://www.7shield.eu/project/>) gives information about 7SHIELD context, objectives and challenges.



#### What is our project ?

SHIELD – Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats is funded by the European Commission (EC) through the [Horizon 2020](#) research and innovation programme, in response to the call 'H2020-SU-INFRA-2019 – Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe'.

Through an innovative approach and thanks to a Consortium of world-leading technical partners, critical infrastructure operators and representatives of Law Enforcement Agencies (LEAs), 7SHIELD's ambition is to provide a holistic framework against Cyber/Physical threats for European Space Ground Segments resilience.

#### The Cyber/Physical threats

In the European new security landscape, ground segments increasingly appear as potential "new targets" for "new threats", especially the hybrid ones (e.g. cyber-physical). A physical/cyber-attack to their installations or communication networks, respectively, would cause debilitating impact on public safety and security of European citizens and affect also other European critical infrastructure. On the one hand, a physical attack on a space ground segment makes the distribution of satellite data problematic and, on the other hand, a cyber-attack in its data storage, access and exchange affects not only the reliability of space data, but also their FAIR standards: findability, accessibility, interoperability and reusability.

Current approaches do not fully exploit the recent advances in surveillance mechanisms with robotic technologies and AI. Moreover, the centralised storage of large streams of space data may result to vulnerable system design, when authentication and single sign on (SSO) is not ensured.

#### 7SHIELD challenge

7SHIELD aims at providing a holistic framework enable to confront complex threats by covering all the macrostages of crisis management, namely pre-crisis, crisis and post-crises phases.

Specifically, the early warning mechanism estimates the level of risk before the occurrence of a cyber or physical attack. During an attack, the detection and response is effective and efficient, taking into account budgetary constraints. A mitigation plan is designed and automatically updated to offer a quick recovery after an intentional attack or a system failure. Security and resilience of private installations of space ground segments are also supported by business continuity scenarios, building on top of an innovative orchestration of novel monitoring and forecasting technologies.

Figure 3-9 - 7SHIELD Project page

### 3.4.1. Concept page

The CONCEPT page (<https://www.7shield.eu/concept/>) gives information on 7SHIELD concept and how 7SHIELD consortium intends to overcome the challenges at stake. The page also contains an illustration of the overall approach.



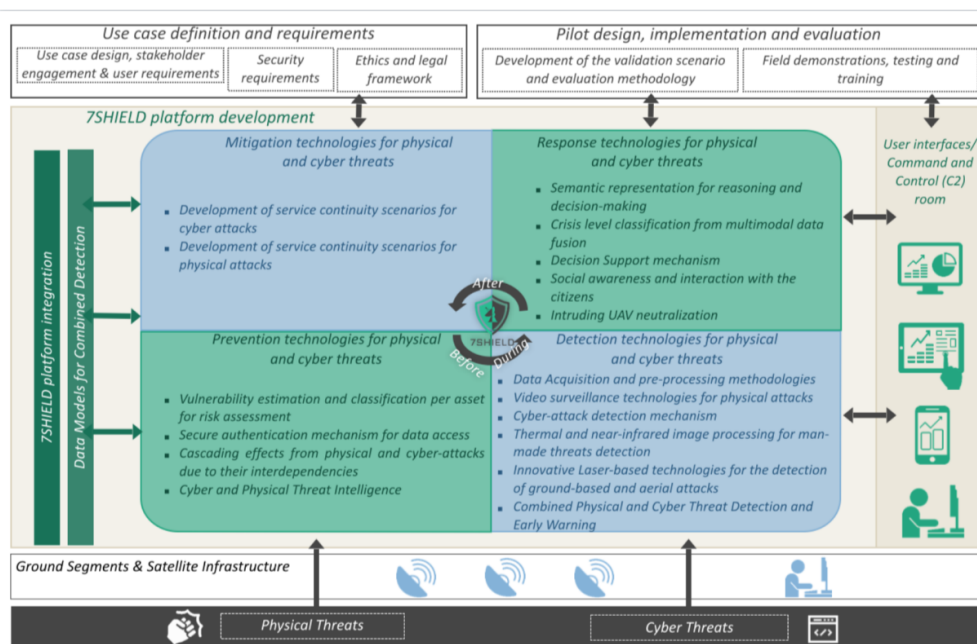
## What is the concept ?

The overall concept of 7SHIELD is to provide to the European Ground Segment facilities a holistic framework enable to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely pre-crisis, crisis and post-crises phases.

7SHIELD integrates a series of state-of-the-art technological achievements from multidisciplinary fields, namely:

- Sensors technologies
- IoT
- Semantic reasoning
- High-level analytics
- Decision support systems
- Crisis management
- Situational awareness

All these technologies will focus on the protection of critical infrastructures such as ground segments of space systems.



The data obtained from 7SHIELD' sensor networks and those from the existing infrastructure of the ground segments themselves will be processed by the innovative threat detection algorithms and high-level multimodal fusion techniques. By utilising bespoke visual analytics tools the outcome will be presented to operators via the 7SHIELD's interactive User Interface.

Practitioners from security sector, first responders and utility providers will be enabled to employ the 7SHIELD's Early Warning and Decision Support System, which also incorporates functionalities for monitoring hazardous circumstances.

Figure 3-10 - 7SHIELD Concept page (abstract)

### 3.4.2. Outcome page

The OUTCOME page (<https://www.7shield.eu/outcome/>) introduces 7SHIELD expected results and gives an overview of each key result (technology brick) that will be developed during the project. The page will be completed and updated throughout the project depending on the key results produced, merged etc.



## A holistic framework against Cyber/Physical threats

7SHIELD result will be an integrated yet flexible and adaptable framework enabling the deployment of innovative services for cyber-physical protection of ground segments, such as e-fences, passive radars and laser technologies, multimedia AI technologies from CCTV cameras and UAVs, that

- Enhance their protection capabilities
- Integrate or interoperate with existing protection solutions already deployed at their installations, EU, national and other systems.

The framework will be open and will integrate advanced state-of-the-art technologies for data integration, processing, and analytics, machine learning and recommendation systems, data visualization and dashboards, data security and cyber threat protection and cyber-attack detection.

The technological solution is co-designed with first responders' teams and contributes to policy making, standardisation and new guidelines for contingency planning. Social awareness is analysed and automatic messages are generated to the public.

The project will be evaluated and demonstrated in five installations of space ground segments through the performance of corresponding pilot use case scenarios.

## Key results

7SHIELD framework will integrate 17 key results (technology bricks) that will be developed and refined during the project.

## Prevention technologies

**Risk assessment tools**  
Description  
[// LEARN MORE >](#)

**Secure authentication mechanism**  
Description  
[// LEARN MORE >](#)

**Combined threat assessment tool**  
Description  
[// LEARN MORE >](#)

**Cyber and Physical Threat Intelligence**  
Description  
[// LEARN MORE >](#)

## Detection technologies

**Data collection and edge processing module**  
Description  
[// LEARN MORE >](#)

**Face detection and face recognition module**  
Description  
[// LEARN MORE >](#)

**Video-based object and activity recognition**  
Description  
[// LEARN MORE >](#)

**Cyber attack detection framework**  
Description  
[// LEARN MORE >](#)

Figure 3-11 - 7SHIELD Outcome page (abstract)



The PILOTS page (<https://www.7shield.eu/our-pilots/>) introduces the 5 partners that will implement all of parts of 7SHIELD framework on their infrastructures. It also illustrates the evaluation cycles that will be implemented with operational tests and demonstrations throughout the project.



# Pilot Use Cases



### 3.5.1. Pilot Use Case pages

Each of the 5 Pilot Use cases is described in a dedicated Pilot Use Case page. These pages are named as following:

- CYBER/PHYSICAL ATTACK IN DEIMOS GROUND SEGMENT – SPAIN  
(<https://www.7shield.eu/pilots/attack-in-deimos-ground/>)
- CYBER/PHYSICAL ATTACK IN NOA GROUND SEGMENT – ATHENS, GREECE  
(<https://www.7shield.eu/pilots/segment-of-noa/>)
- CYBER ATTACK ON ONDA DIAS PLATFORM  
(<https://www.7shield.eu/pilots/onda-dias-platform/>)
- THREAT DETECTION & MITIGATION ON THE ICE CUBES SERVICE  
(<https://www.7shield.eu/pilots/ice-cubes-service/>)
- PHYSICAL ATTACK IN ARTIC SPACE CENTER – SODANKYLA, FINLAND  
(<https://www.7shield.eu/pilots/arctic-space-centre/>)

Each Pilot Use Case page describes:

- the infrastructure(s) on which 7SHIELD framework will be tested;
- the simulated attack scenario upon which 7SHIELD framework will be tested;
- 7SHIELD potential future outcomes for the partner and its specific infrastructure(s).

Each Pilot Use Case page also contains an illustration of the infrastructure that will implement the pilot.

# CYBER ATTACK ON ONDA DIAS PLATFORM



Image provided by jcomp – it.freepik.com

## Critical Infrastructure

ONDA by Serco® is a registered trademark of Serco Italia S.p.A. and is one of the five ESA Data and Information Access Services (DIAS). Serco is responsible for ONDA operations and services and is the contractual entity leading with ONDA end-users.

## Motivation

A Space mission Ground Segment represent the set of infrastructure, equipment and functions to allow the processing, archiving and dissemination of Satellite data. The data archiving function in particular has the objective to store and preserve the mission products for the long term (i.e. a longer period than the contractual coverage of the activity). The infrastructure security problem is therefore largely impacting the performance of the afore-mentioned services but it may have critical impacts especially on Data Access and Long-Term Archive service. Indeed, in case of a major attack causing the unavailability of these services, the performance of the entirely mission is affected: e.g. in case of Data Access unavailability the users cannot have access to satellite data. The cyber-security attack scenario is drastically enlarging the impact within the EU Copernicus Programme (<https://www.copernicus.eu/en>). As a pilot for our project, we selected the ONDA DIAS cloud infrastructure (<https://www.onda-dias.eu/cms/>) to exploit cyber-security scenarios. ONDA is the Serco DIAS platform enabling users to host data and to build their applications in the Cloud. We are storing more than 16PB of satellite data from Earth Observation satellites, including the Sentinels – a family of missions developed by ESA for the operational needs of the Copernicus programme – Envisat and Landsat 8 and from Copernicus Services Projects (e.g. Land and the Marine environment monitoring services)

*Figure 3-13 – SERCO's Pilot Use Case page (abstract)*



### 3.6. Report & publications page

The REPORT & PUBLICATIONS page (<https://www.7shield.eu/reports-publications/>) includes 4 tables.

The first table lists all public deliverables, with a link to download the documents in PDF. It indicates for each document:

- its ID (according to the Grant Agreement);
- its title (with a link to download the documents in PDF);
- a short description of the document.

The second table lists all presentations, abstracts and other relevant material. It indicates for each document:

- the date of publication;
- the event for which it was created;
- its title (with a link to download the documents in PDF);
- the author(s).

The third table lists all papers produced in the frame of the project and published in scientific journals.

The fourth table lists all other papers published in conferences.

These two tables indicate for each document:

- the date of publication;
- its title;
- the author(s);
- the link to the paper hosted in scientific databases.

The REPORT & PUBLICATIONS page will be updated every month with the public deliverables, presentations, abstracts, papers and scientific publication produced and validated by the consortium (and the Project Officer in case of public deliverables).

# Reports & publications

## Deliverables

Public deliverables produced in the frame of 7SHIELD work programme are available here:

ID	Title	Short description

## Presentations

Presentations, abstract and other relevant material of 7SHIELD project are available here:

Date	Event	Material	Author(s)

## Scientific publications

Papers published in scientific journals are available here:

Date	Title	Author(s)	Link

## Papers

Papers published in conferences are available here:

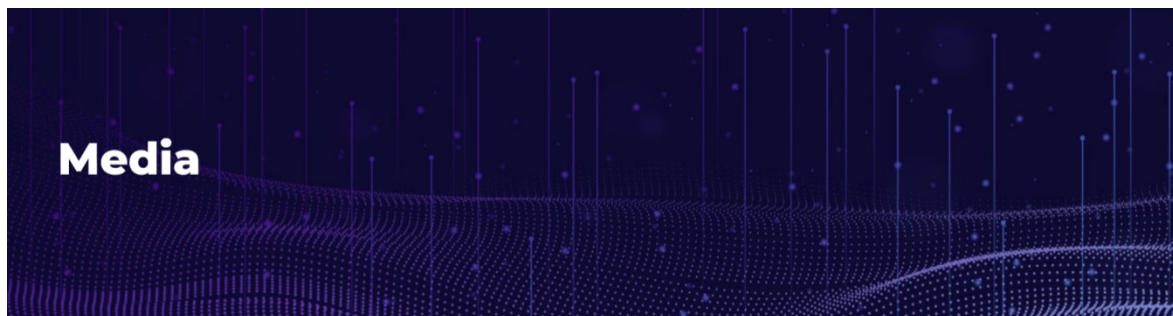
Date	Title	Author(s)	Link

Figure 3-14 - 7SHIELD Reports & publications page

### 3.7. Media page

The MEDIA page (<https://www.7shield.eu/media/>) gives access to 7SHIELD communication kit, i.e. a set of communication materials to be downloaded by anyone wishing to communicate about 7SHIELD. It is composed of 7SHIELD official logo, and will be enhanced throughout the project with a commercial presentation, a brochure, an info board and a video.

The page also includes a list of each article from external media referring to 7SHIELD, with a link to the article.



#### 7SHIELD communication kit

7SHIELD communication materials are available here:

Date	Title	Format	Link
05/11/2020	7SHIELD Logo	PNG	<a href="#">7shield-logo</a>

#### 7SHIELD in other media

Articles, interviews and references to 7SHIELD project have been made in several media, which are listed below:


- <https://www.agendadigitale.eu/sicurezza/cybersecurity-e-lo-spazio-la-nuova-frontiera-leuropa-schiera-7shield/>

Figure 3-15 - 7SHIELD Media page

### 3.8. Consortium page


The CONSORTIUM page (<https://www.7shield.eu/consortium/>) introduces the 22 partners of 7SHIELD consortium with, for each organisation:

- its logo;
- its name;
- its nature (Private company, Research centre etc.);
- a short description;
- a link to the page dedicated to the partner.



**7SHIELD consortium**

7SHIELD consortium is composed of 22 partners from 12 different countries. It includes Private companies, Centres of excellence, Research & technology centres, Regulation authorities, Meteorological Institutes, Law enforcements and Research foundations. This multidisciplinary approach enables 7SHIELD to cover all the crisis management steps, test and demonstrate its solutions directly on partners' infrastructures.



### Consortium partners







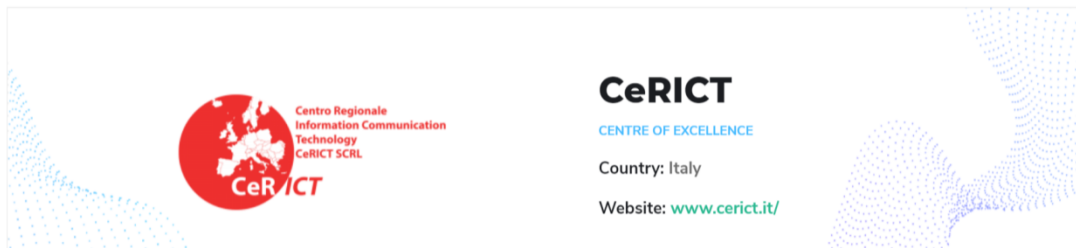
 <b>ACCELOGENCE LTD</b> Private company  Cyprus-based company, established in 2019 . ACCELOGENCE Ltd. is engaged in cutting edge R&D activities in order to boost innovation capital, improve products and ensure alignment of the services to the state of the art. <a href="#">→ LEARN MORE</a>	 <b>CENTRIC</b> Centre of excellence  CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence & Organised Crime Research) is a multidisciplinary, security-focused research centre located at Sheffield Hallam University. <a href="#">→ LEARN MORE</a>	 <b>CeRICT</b> Research Consortium  CeRICT ( <a href="http://www.cerict.it/">http://www.cerict.it/</a> ) is a research consortium founded in 2005 as a no-profit organization to foster the cooperation of Italian computer scientists and engineers in nation-wide and international projects in the area of Information and Communication Technology (ICT). <a href="#">→ LEARN MORE</a>
 <b>CERTH</b> Research & technology centre  The Centre for Research and Technology-Hellas (CERTH), founded in	 <b>Cyberlens</b> Private company  Cyprus-based company, established in 2019 . ACCELOGENCE Ltd. is engaged in	 <b>CS Group</b> Private company  CS GROUP is a mid-cap company, based in France, with subsidiaries in

Figure 3-16 - 7SHIELD Consortium page

### 3.8.1. Partner pages

Each of the 22 partners has a dedicated page accessible from the Consortium page. Each page gives information on the organisation (logo, name and nature of the organisation, country and website), a description of the partner main activities, its role in 7SHIELD project and the key results it will develop during the project.

For example, CeRICT's dedicated page is accessible at <https://www.7shield.eu/cerict/>.



## Description

CeRICT (<http://www.cerict.it/>) is a research consortium founded in 2005 as a no-profit organization to foster the cooperation of Italian computer scientists and engineers in nation-wide and international projects in the area of Information and Communication Technology (ICT). It currently comprises eight partners, and precisely: universities (among which the University of Naples Parthenope), the Consorzio Interuniversitario Nazionale per l'Informatica (CINI), Consiglio Nazionale delle Ricerche (CNR), and the Pascale Foundation.

The Research Team which will be contributing to this proposal is the Fault and Intrusion Tolerant Networked SystemS (FITNESS) Research Group (<http://www.fitnesslab.eu/>), which consists of researchers who are currently at the University of Naples Parthenope. These researchers have been actively involved in several EU-funded projects.

## Role in the project

CeRICT will be in charge of coordinating the research work related to Intrusion Detection mechanisms and cyber-attack detection methods. It will also participate in the design and integration of the overall platform. Finally, CeRICT will contribute to the development of the validation scenarios, the evaluation methodology, and the actual validation of project results.

Figure 3-17 – CeRICT's individual page

### 3.9. News & Events page

The NEWS & EVENTS (<https://www.7shield.eu/blog/>) page lists all the articles published by 7SHIELD communication team on the website and LinkedIn page during the project. Full articles are accessible by clicking on the article snippets on the page.

Links to Newsletters page and Events pages are available on the right of the page.

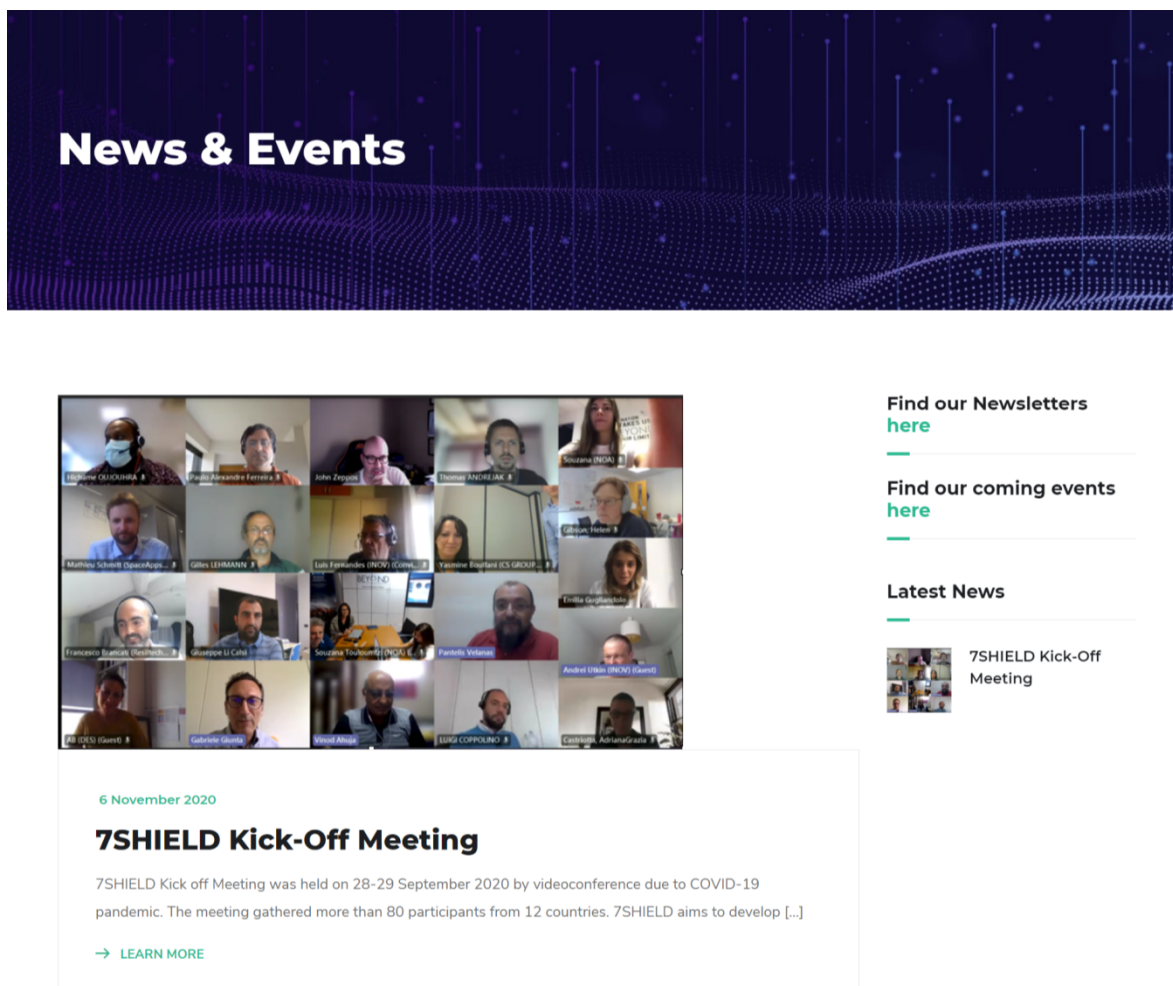


Figure 3-18 - 7SHIELD News & Events page

3.9.1. Newsletters page

The NEWSLETTERS (<https://www.7shield.eu/newsletters/>) page gives access to the newsletters that will be published every year during the project. PDF versions of the newsletters will be accessible through a download link.



7SHIELD newsletters are available here:

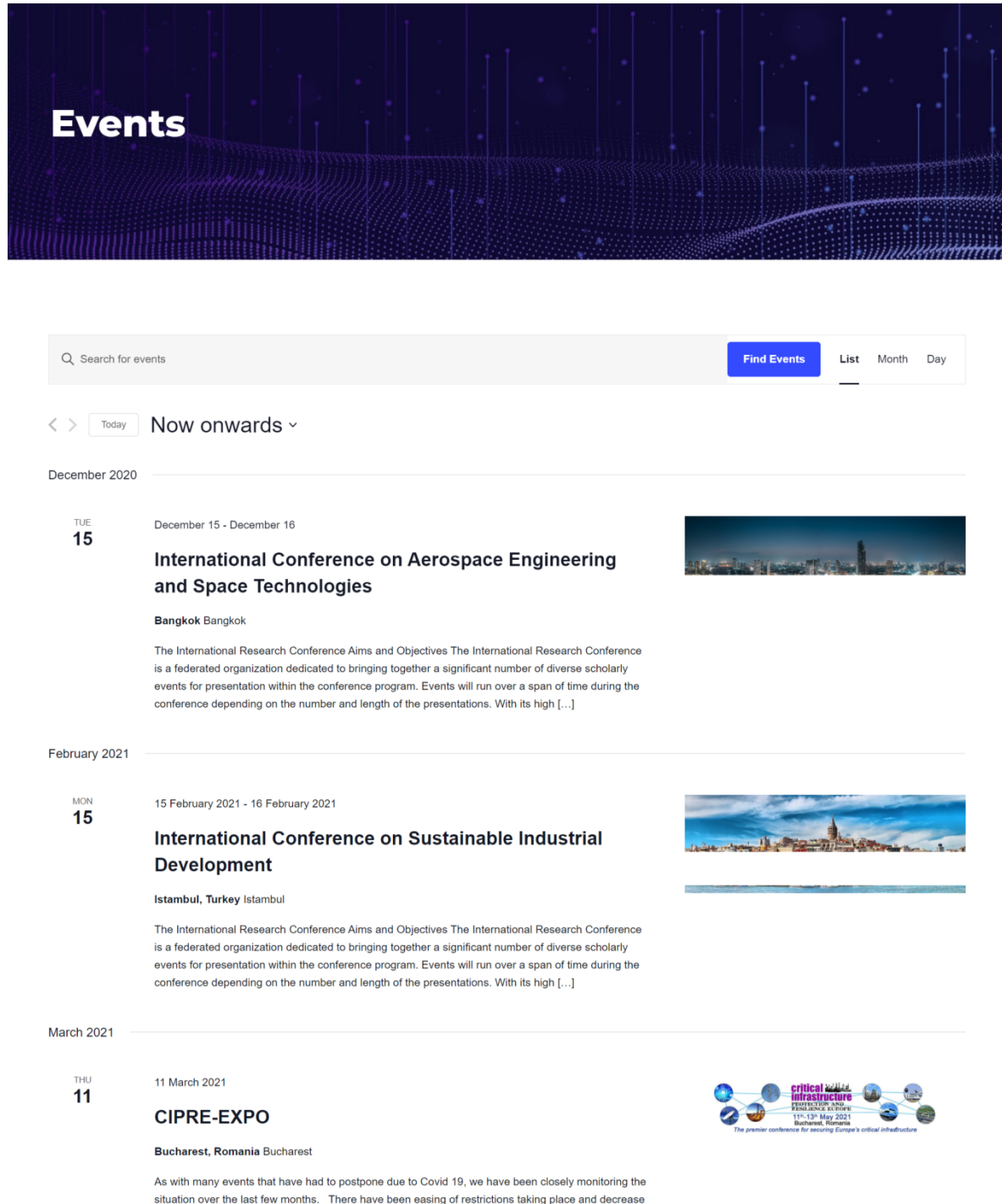
Date	Title	Link

Figure 3-19 - 7SHIELD Newsletters page



### 3.9.2. Events page

The EVENTS page (<https://www.7shield.eu/events/>) lists all the past and coming events to which members of 7SHIELD consortium participate and that are related to 7SHIELD activities. It could be external events or events organised within the frame of 7SHIELD activities.



The screenshot displays the 'Events' page of the 7SHIELD website. The header features a dark blue background with a network-like pattern and the word 'Events' in white. Below the header is a search bar with the placeholder text 'Search for events' and a 'Find Events' button. To the right of the search bar are tabs for 'List', 'Month', and 'Day'. The main content area shows a calendar view for 'Now onwards'. The first event listed is the 'International Conference on Aerospace Engineering and Space Technologies' in Bangkok, scheduled for December 15-16, 2020. The second event is the 'International Conference on Sustainable Industrial Development' in Istanbul, Turkey, scheduled for February 15-16, 2021. The third event is 'CIPRE-EXPO' in Bucharest, Romania, scheduled for March 11, 2021. Each event entry includes a date, a title, a location, and a brief description. The 'CIPRE-EXPO' entry also includes a small graphic with the text 'critical infrastructure' and '11th-13th May 2021 Bucharest, Romania'.

Figure 3-20 - 7SHIELD Events page (abstract)



### 3.9.3. Links page

The LINKS page (<https://www.7shield.eu/links/>) lists all institutions, EO organisations, major stakeholders and other relevant projects that are linked to 7SHIELD project. It includes links to the website of each identified organisation.



#### Links to institutional websites

Name	Description
<a href="#">European Commission</a>	The executive body of the European Union
<a href="#">Europe 2020 strategy</a>	The EU agenda for growth and jobs for the current decade
<a href="#">Innovation Union</a>	The EU strategy to create an innovation-friendly environment bringing economy growth and jobs
<a href="#">HORIZON 2020</a>	The EU Framework Programme for Research and Innovation – The financial instrument implementing the Innovation Union
<a href="#">CORDIS</a>	Community Research and Development Information Service – The EC portal disseminating the results of EU research and innovation
<a href="#">research*eu</a>	Magazine covering specific topics of research interest from EU-funded projects
<a href="#">OpenAIRE</a>	Open Access Infrastructure for Research in Europe

#### Link to EO Organisations – Stakeholders

Name	Description
<a href="#">GEOSS</a>	The Global Earth Observation System of Systems
<a href="#">GEO</a>	The Group on Earth Observations
<a href="#">EARS</a>	the European Association of Remote Sensing Companies
<a href="#">CEOS</a>	the Committee of Earth Observation Satellites

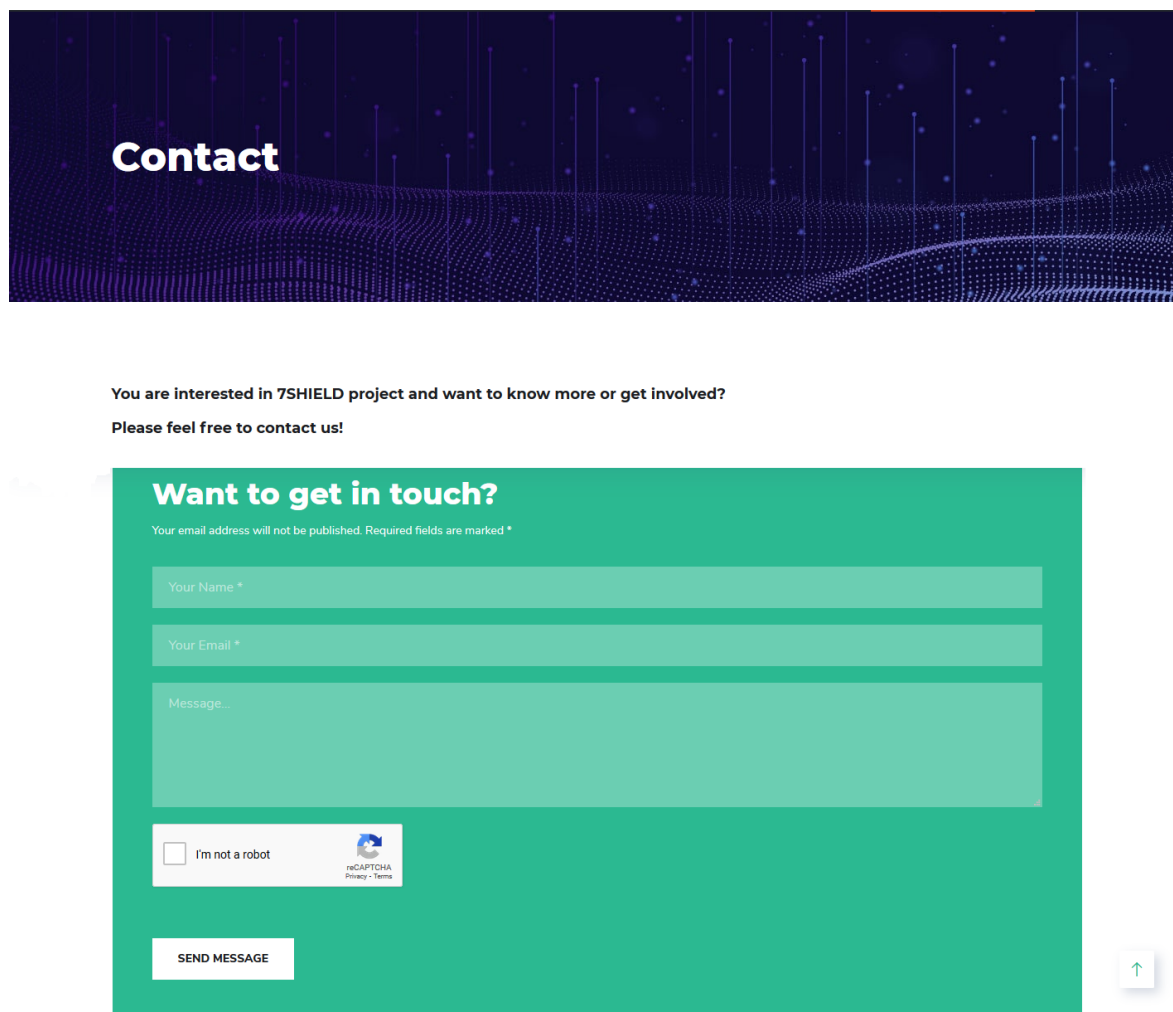
#### Link to other relevant projects

Name	Description
<a href="#">H2020 - SAFECARE</a>	Focusing on health services infrastructure, SAFECARE will work towards creating a global protection system, which will cover threat prevention, detection, response and mitigation of impacts across infrastructures, populations and environments.
<a href="#">H2020 - InfraSTRESS</a>	INFRASTRESS addresses cyber-physical (C/P) security of Sensitive Industrial Plants and Sites (SIPS) Critical Infrastructures (CI) and improves resilience and protection capabilities of SIPS exposed to large scale, combined, C/P threats and hazards, and guarantee continuity of operations, while minimising cascading effects in the infrastructure itself, the environment, other CIs, and citizens in vicinity.
<a href="#">H2020 - SecureGas</a>	SecureGas focuses on the 140.000Km of the European Gas network covering the entire value chain from Production to Distribution to

Figure 3-21 - 7SHIELD Links page (abstract)

### 3.10. Contact page

The CONTACT page (<https://www.7shield.eu/contact/>) includes a contact form enabling external organisations to get in touch with 7SHIELD consortium members.



The screenshot shows the 7SHIELD Contact page. At the top, there is a dark blue header with the word "Contact" in white. Below the header, the text reads: "You are interested in 7SHIELD project and want to know more or get involved? Please feel free to contact us!". The main content area is a green box titled "Want to get in touch?". Inside this box, there is a disclaimer: "Your email address will not be published. Required fields are marked \*". The form contains three input fields: "Your Name \*", "Your Email \*", and a larger "Message..." text area. Below these fields is a reCAPTCHA widget with the text "I'm not a robot" and a "SEND MESSAGE" button. A small upward arrow icon is located at the bottom right of the green box.

Figure 3-22 - 7SHIELD Contact page

## 4. Website strategy

7SHIELD website is a tool made to support the consortium members in their communication and dissemination activities. It will help them reach their objectives regarding events participation, stakeholders involvement, public awareness, results dissemination and exploitation and 7SHIELD overall impacts.

In order to improve the quality and quantity of the traffic, 7SHIELD website follows several Search Engine Optimisation principles:

- Each page title includes relevant tags
- Each page is focused on one specific topic
- The page loading speed is optimised through image compressing and content caching
- The navigation menu stays simple and intuitive
- The pages contain as much relevant illustrations as possible
- Each page contains links to other pages of the website
- The website contains links to relevant external websites

The website will be updated every month with news about on-going activities, achieved objectives, results, coming events etc. All partners will participate in the elaboration of this news.

To increase 7SHIELD website visibility toward external audiences, all partners will be asked to put on their own websites a link toward 7SHIELD website.

The main audiences targeted by 7SHIELD website are listed above. They have been identified both regarding their potential interest in the project activities & results and regarding the potential benefits the consortium members could derive from interactions with these audiences.

Target Group	Examples/ Representative Organisations
Space Agencies, Organisations of space agencies	<ul style="list-style-type: none"><li>• Committee of Earth Observation Satellites (CEOS)</li><li>• Agenzia Spaziale Italiana (ASI), Italy</li><li>• Canadian Space Agency (CSA), Canada</li><li>• Center for the Development of Industrial Technology (CDTI), Spain</li><li>• Centre National d'Etudes Spatiales (CNES), France</li><li>• Comisión Nacional de Actividades Espaciales (CONAE), Argentina</li><li>• Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia</li><li>• Deutsches Zentrum für Luft-und Raumfahrt (DLR), Germany</li></ul>

	<ul style="list-style-type: none"> <li>• European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT), Germany</li> <li>• European Space Agency (ESA), Europe</li> <li>• European GNSS Agency (GSA), Europe</li> <li>• Instituto Nacional de Pesquisas Espaciais (INPE), Brazil</li> <li>• Aerospace Exploration Agency/Ministry of Education, Culture, Sports, Science, and Technology (JAXA/MEXT), Japan</li> <li>• National Aeronautics &amp; Space Administration (NASA), USA</li> <li>• National Oceanic and Atmospheric Administration (NOAA), USA</li> <li>• National Space Agency of Ukraine (NSAU), Ukraine</li> <li>• Netherlands Space Office (NSO), Netherlands</li> <li>• United Arab Emirates Space Agency (UAE SA), United Arab Emirates</li> <li>• United Kingdom Space Agency (UKSA), United Kingdom</li> <li>• Global Climate Observing System (GCOS), Switzerland</li> <li>• Swedish National Space Agency (SNSA), Sweden</li> </ul>
Commercial operators of Satellite Ground Segments	<ul style="list-style-type: none"> <li>• Airbus DS Geo, France</li> <li>• Telespazio, Italy</li> <li>• Collecte Localisation Satellites (CLS), France</li> <li>• Planet, USA</li> <li>• Digital Globe, (MAXAR) USA</li> <li>• GeoEye, USA</li> <li>• ATOS, Spain</li> </ul>
Commercial operators of telecommunication Satellite Ground Segments	<ul style="list-style-type: none"> <li>• SES, Luxembourg</li> <li>• Intelsat, Luxembourg</li> <li>• Eutelsat, France</li> <li>• Avantiplc, UK</li> <li>• Inmarsat, UK</li> <li>• Kongsberg Satellite Services (KSAT), Norway</li> <li>• Hellas Sat, Greece</li> <li>• Swedish Space Corporation (SSC), Sweden,</li> <li>• Hispasat, Spain</li> </ul>
National and Regional Meteorological Institutes	<ul style="list-style-type: none"> <li>• European Centre for Medium-Range Weather Forecasts (ECMWF), Europe</li> <li>• Finnish Meteorological Institute (FMI), Finland</li> <li>• Météo-France, France</li> <li>• Institut Royal Météorologique (IRM), Belgium</li> <li>• The Royal Netherlands Meteorological Institute (KNMI), Netherlands</li> <li>• Instituto Portugues do Mar e da Atmosfera (IPMA), Portugal</li> <li>• Meteorologisk Institutt, Norway</li> </ul>

	<ul style="list-style-type: none"> <li>• Deutscher Wetterdienst, Germany</li> <li>• Hellenic National Meteorological Service, Greece</li> <li>• Ufficio Generale Spazio Aereo e Meteorologia, Italy</li> <li>• Agencia Estatal de Meteorología (AEMET), Spain</li> <li>• Swedish Meteorological and Hydrological Institute, Sweden</li> <li>• Met Office, UK</li> <li>• MétéoSuisse, Switzerland</li> </ul>
EO platform operators	<ul style="list-style-type: none"> <li>• SERCO, Italy</li> <li>• Airbus Defence &amp; Space, France</li> <li>• Creotech Instruments, Poland</li> <li>• Atos, France</li> <li>• E-Geos, Italy</li> </ul>
Manufacturers of systems for Satellite Ground Segment	<ul style="list-style-type: none"> <li>• GMV</li> <li>• RHEA group</li> <li>• TERMA</li> <li>• A more complete list can be found here: <a href="https://spaceindustrydatabase.com/">https://spaceindustrydatabase.com/</a></li> </ul>
European Association of Remote Sensing Companies (EARSC)	<ul style="list-style-type: none"> <li>• Airbus, France</li> <li>• ALPHA Consult, Italy</li> <li>• Ariespace, Italy</li> <li>• EOAnalytics, Ireland</li> <li>• European Space Imaging, Germany</li> <li>• Geospatial Enabling Technologies, Greece</li> <li>• HISDESAT, Spain</li> <li>• ICEYE, Finland</li> <li>• Kongsberg Spacetec, Norway</li> <li>• Neuropublic, Greece</li> <li>• Planet Germany, Germany</li> <li>• Planetek Hellas, Greece</li> <li>• SpaceSeed, France</li> <li>• SuperVision Earth, Germany</li> <li>• Thales Alenia Space, France</li> <li>• Draxis SA, Greece</li> </ul>
Civil Protection Agencies / Governmental Bodies	<ul style="list-style-type: none"> <li>• General Secretariat for Civil Protection, Greece</li> <li>• Dipartimento della Protezione Civile, Italy</li> <li>• Directorate General of Civil Protection and Emergencies, Spain</li> <li>• Civil Defence, Ministry of Interior, Cyprus</li> </ul>
CI Operators, Ministries & CI Protection Agencies	<ul style="list-style-type: none"> <li>• Finnish Transport Infrastructure Agency, Finland</li> <li>• Ministry of Infrastructure and Water Management, Netherlands</li> <li>• National Infrastructure Commission, UK</li> <li>• Swiss Civil Protection</li> </ul>

	<ul style="list-style-type: none"> <li>Water Board of Nicosia, CY</li> </ul>
Cybersecurity Agencies	<ul style="list-style-type: none"> <li>European Union Agency for Cybersecurity (ENISA)</li> <li>European Cyber Security Organisation: ECSO</li> <li>European Organisation for Security (EOS)</li> </ul>
Defence Agencies	<ul style="list-style-type: none"> <li>European Defence Agency (EDA)</li> </ul>
General Public	<ul style="list-style-type: none"> <li>All European Citizens</li> </ul>

4-1 - Main target audiences of the 7SHIELD website

The consortium has defined several KPIs and audience objectives regarding 7SHIELD website and its targeted audiences:

Metric	Target
Website audience	10 000 visits over the 2-year project +20% visits each year
Downloads of online material (communication kit, public deliverable, scientific publication etc.)	300 downloads over the 2-year project

4-2 - 7SHIELD website KPIs

Analytics tools such as Google Analytics will be used to collect insight on the website visibility and traffic. In particular, it will be used to analyse which webpages have the most visits, which content is being read or downloaded, how users reach the website and how they interact with its pages and content. An internal report on audience statistics will be generated and shared among the consortium members every month.

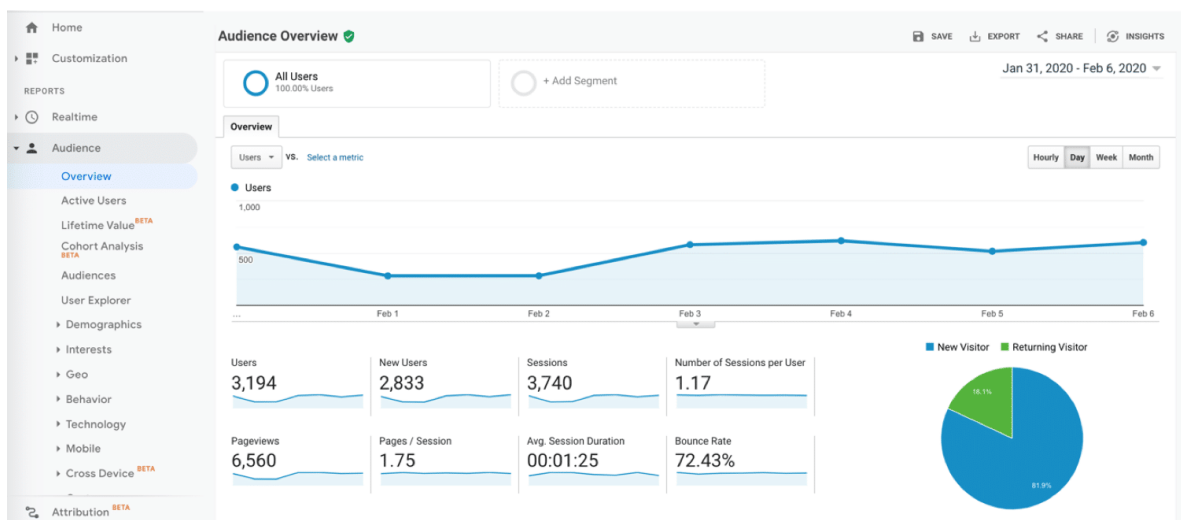


Figure 4-1 - Analytic report on 7SHIELD website audience



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