
# D8.1 Communication and dissemination plan

| | |
|---|---|
| **Work Package:** | WP8 Dissemination, Impact Creation and Exploitation Plan |
| **Lead partner:** | National Observatory of Athens (NOA) |
| **Author(s):** | Ioannis Papoutsis (NOA), Souzana Touloumtzi (NOA), Alkyoni Baglatzi (NOA), Dimitris Sykas (NOA), Gabriele Giunta (ENG), Gilles Lehmann (CSNov), Leslie Gale (SPACEAPPS), Franck Ranera (SERCO), Adriana Grazia Castriotta (SERCO), Sandra Negrin (DEIMOS), Ana Barba (DES), Panagiotis Nikolaidis (HP), Agathi Barmpaki (KEMEA), Ilias Gkotsis (KEMEA), Xavier Pothrat (CS), John Zeppos (RG), Vassilios Argyroulis (EETT), Pantelis Velanas (ACCELI), Gerasimos Antzoulatos (CERTH) |
| **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 1st, 2020 |
| **Duration:** | 24 months |
| **Call identifier:** | H2020-SU-INFRA-2019 |
| **Topic:** | SU-INFRA01-2018-2019-2020<br>Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe |
| **Instrument:** | IA |

Horizon 2020 European Union Funding for Research & Innovation

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

# Revision History

| Revision | Date | Who | Description |
|---|---|---|---|
| 0.1 | 11/11/2020 | NOA | First release of the communication and dissemination plan |
| 0.2 | 17/11/2020 | NOA | Incorporation of partners' input |
| 0.3 | 18/11/2020 | NOA | Incorporation of SERCO input |
| 0.4 | 24/11/2020 | NOA | Draft submitted for Quality Control |
| 0.5 | 27/11/2020 | NOA | Release of final deliverable |
| 1.0 | 27/11/2020 | ENG | Final version |

# Quality Control

| Role | Date | Who | Approved/Comment |
|---|---|---|---|
| Internal review | 25/11/2020 | DES | Approved |
| Internal review | 25/11/2020 | CSNov | Approved |

# Related deliverables

| ID | Title | Lead partner | Dissemination level |
|---|---|---|---|
| D1.1 | Project management and quality assurance plan | ENG | Confidential |
| D8.2 | Corporate identity and logo | CS | Public |
| D8.3 | Project website | CS | Public |

# 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 Communication and Dissemination plan sets forth the project's outreach strategy, identifying the appropriate target groups and defining means to reach and involve them in 7SHIELD activities throughout the project duration and beyond.

It will be a living, evolving document, which will include updates on how the project communicates with key targets so as to ensure the long-lasting visibility of 7SHIELD after its closure. Specifically, this document includes the information needed to facilitate the communication and dissemination efforts of 7SHIELD partners, defining, among others, the communication objectives, the key messages addressed to each target audience, the development of appropriate online channels (social media pages, website, e-newsletters), the design of printed materials, the content and frequency of communication and dissemination activities, the organization of networking activities and participation in third-party events, as well as synergies with relevant H2020 projects and foreseen scientific publications. Lastly, the document provides basic guidelines to the partners for compliance with the rules for visibility of EU funding, data protection regulations, and security considerations applying to the project's publications.

# Table of Contents

# List of figures



# List of Tables

# Definitions and acronyms

| | |
|---|---|
| AMGA | Annotated Model Grant Agreement |
| CA | Consortium Agreement |
| CI | Critical Infrastructure |
| CIP | Critical Infrastructure Protection |
| CM | Communication Manager |
| C/P | Cyber/Physical |
| DoA | Description of Action |
| EC | European Commission |
| EO | Earth Observation |
| EU | European Union |
| GA | Grant Agreement |
| GDPR | General Data Protection Regulation |
| GS | Ground Segment |
| GSSS | Ground Segments of Space Systems |
| ICT | Information and Communications Technology |
| IoT | Internet of Things |
| KPI | Key Performance Indicator |
| KR | Key Result |
| PC | Project Coordinator |
| PCT | Project Communication Team |
| PMB | Project Management Board |
| PSO | Project Security Officer |
| SAB | Security Advisory Board |
| SC | Scientific Coordinator |
| SGS | Satellite Ground Station |
| SGSA | Satellite Ground Station Assets |
| SMEs | Small and Medium-size Enterprises |
| TM | Technical Manager |
| UAV | Unmanned Aerial Vehicle |
| WP | Work Package |

# 1. Introduction

## 1.1. The 7SHIELD project

The project aims to address the security and resilience of EU Ground Segments of Space Systems, in response to the European Union's call for prevention, detection, response and mitigation of combined physical and cyber threats to Critical Infrastructure in Europe.

A physical and/or cyber-attack can have far reaching consequences impacting the assets of the ground system itself or the assets that are managed, controlled and exploited by the ground segment system. New markets have been created by the realisation of Copernicus massive amounts of satellite data that the Ground Segments of Space Systems receive are used to serve the industry and governmental bodies. A cyber or physical attack to the ground segment installations or communication networks would cause debilitating impact on public safety and security of EU citizens and public authorities. A physical attack on a space ground segment would make the distribution of satellite data problematic and, on the other hand, a cyber-attack in its data storage, access and exchange would affect the reliability, accessibility, interoperability and reusability of the data. An attack on other ground segment systems that operate assets onboard satellites or platforms such as the International Space Station and in the future in lunar orbit on the moon or further into space can result in the loss or misuse of the asset, compromising its objectives and, potentially, in the case of the International Space Station and similar facilities threaten the safety of astronauts. Although it must be stressed that such systems are subject to extreme evaluation, review and testing, aimed at guaranteeing that the asset safely operates under all circumstances.

The innovation of 7SHIELD lays on the fact that there is evidence that current approaches in cyber-physical security of critical EU Ground Segments of Space Systems do not fully exploit the recent advances in surveillance and detection mechanisms with robotic technologies and Artificial Intelligence. 7SHIELD brings together 22 partners (Table 1-1) from 12 European countries (Figure 1-1) to design and develop an integrated, flexible and adaptable framework enabling the deployment of innovative services for cyber-physical protection of ground segments, such as e-fences, multimedia AI technologies, passive radars and laser technologies to enhance the protection capabilities of the ground segments while integrating or interoperating with existing protection solutions already deployed at their installations.

The envisioned framework will integrate advanced technologies for data integration, processing, and analytics, machine learning and recommendation systems, data visualization and dashboards, data security and cyber threat protection. The 7SHIELD platform is co-designed with first responders' teams and will contribute to policy making, standardisation and new guidelines for contingency planning and service continuity. The platform will be evaluated and demonstrated in five installations of Ground Segments of Space Systems in Italy, Finland, Spain, Greece, and Belgium.


*Figure 1-1 Geographical coverage of the 7SHIELD Consortium*

| No | Partner Name | Short Name | Country |
|---|---|---|---|
| 1 | Engineering – Ingegneria Informatica SpA | ENG | Italy |
| 2 | Centre for Research & Technology Hellas | CERTH | Greece |
| 3 | Space Applications Services NV | SPACEAPPS | Belgium |
| 4 | Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research | CENTRIC | United Kingdom |
| 5 | Serco Italia SpA | SERCO | Italy |
| 6 | Finnish Meteorological Institute | FMI | Finland |
| 7 | National Observatory of Athens | NOA | Greece |
| 8 | Inov Inesc Inovação – Instituto de Novas Tecnologias | INOV | Portugal |
| 9 | Satways Ltd | STWS | Greece |
| 10 | CS Systèmes d'Information SA | CS | France |
| 11 | Deimos Space Sociedad Limitada Unipersonal | DEIMOS | Spain |
| 12 | Deimos Engineering and Systems SLU | DES | Spain |
| 13 | Dr Frucht Systems Ltd | DFSL | Israel |
| 14 | Resilience Guard GmbH | RG | Switzerland |
| 15 | Hellenic Telecommunications and Post Commission | EETT | Greece |
| 16 | Centre for Security Studies | KEMEA | Greece |
| 17 | Acceligence Ltd | ACCELI | Cyprus |
| 18 | Resiltech Srl | RESIL | Italy |

| | | | |
|---|---|---|---|
| 19 | Hellenic Police | HP | Greece |
| 20 | Regional Centre on Information Communication Technology scrl | CeRICT | Italy |
| 21 | Cyberlens BV | CLS | Netherlands |
| 22 | CS Novidy's | CSNov | France |

*Table 1-1 The 7SHIELD Consortium*

## 1.2. Description of the deliverable

This document presents the Communication and Dissemination strategy of 7SHIELD. It provides the partners with the necessary information and tools to facilitate the effective communication of the project to its target audiences and the proper dissemination of its results.

The deliverable is organised in 7 main chapters:

- Chapter 1 is a brief introduction to the project and the consortium,
- Chapter 2 explains the communication objectives and positioning of 7SHIELD, identifies the primary and secondary target audiences, defines the key communication messages, and clarifies the roles and responsibilities of the Communication Manager and the Project Communication Team,
- Chapter 3 elaborates the communication plan, presenting the online channels that will be developed and used for the promotion of the project and its results, as well as the electronic and printed communication materials. This chapter also provides guidelines for press releases, content and frequency of communication activities,
- Chapter 4 defines the project outputs that will be disseminated and maps the key stakeholders and relevant networking activities, including 7SHIELD and third-party events. The dissemination plan also outlines the synergies with other H2020 projects and relevant initiatives of the space sector, as well as the foreseen scientific publications,
- Chapter 5 provides the tools to measure the project's impact and performance of the communication and dissemination activities,
- Chapter 6 explains the compliance framework of the communication actions, providing the guidelines for the visibility of EU funding, data protection issues and security considerations for the handling of EU Classified Information,
- Chapter 7 provides the overall time plan of activities and partners' involvement in the communication and dissemination tasks,
- Chapter 8 concludes the document.

# 2. Communication & dissemination strategy

## 2.1. Communication objectives & positioning of 7SHIELD

7SHIELD aspires to position itself as a technology enabler that will shield Ground Segments of Space systems, their assets and the associated value chains that exploit the assets, through the integrated analysis of multi-sensor data, historical knowledge on adverse situational factors, domain-specific expertise, and novel ICT.

The communication activities aim to maximise the visibility of 7SHIELD to its target communities and the general public, raise awareness of the need to protect Ground Segments of Space Systems against combined threats, engage stakeholders, and ensure the exploitation of project results during and beyond its lifespan.

Throughout the project, all the Consortium members will systematically perform communication and dissemination actions to achieve the commonly agreed objectives set by the communication and dissemination strategy. These objectives are to:

- **Promote the project** early and effectively, bringing the consortium's research to the attention of multiple specialist and non-specialist audiences, as well as the media, in alignment with the EU guidelines on communicating research and innovation funding,
- **Engage stakeholders** to ensure their active participation in the research activities and their contribution to the production and validation of project results,
- **Build networks** and establish close collaborations with other projects in similar research domains, especially Earth Observation, Remote Sensing, and Security of Critical EU Infrastructure,
- **Raise citizens' awareness** of the imperative to protect EU Critical Infrastructure – and specifically satellite Ground Segment assets – against cyber and physical threats,
- **Inform and influence policymakers**, funding sources, and governmental authorities to standardise strategies and policies for the prevention, detection, response, and mitigation of cyber and physical attacks on space systems' Ground Segments,
- **Maximise participation** to the project's networking events and workshops,
- **Ensure the exploitation** of the project's outputs by potential users,
- **Generate market demand** for the project's Key Results, attracting business partners and potential users of the developed technologies.

The achievement of the communication objectives will be monitored and evaluated during and beyond the project lifecycle, using specific and measurable Key Performance Indicators – KPIs (elaborated in Chapter 5). Depending on the actual results, the communication and dissemination strategy will be adjusted, if necessary, in order to achieve the desired visibility and impact.

## 2.2. Target audiences

The primary target audiences of 7SHIELD are mainly public and private Ground Segments of Space Systems Agencies of different natures but also include other actors of the downstream ecosystem. Other groups (secondary audiences) that will be targeted by the project partners include Remote Sensing companies, researchers in Big Data, Cloud and High Performance Computing, developers and cybersecurity officers, civil protection, governmental and public authorities, and SMEs in the field of public safety and security. The communication activities will also aim to raise European citizens' awareness of the importance of Critical Infrastructure Protection and Security.

Indicative lists of representative organisations and examples per target group, as well as the partners responsible to reach each target group, are provided in the tables in sections 2.2.1 (Table 1-1) and 2.2.2 (Table 2-2).

### *2.2.1. Primary target audiences*

| Target Group | Examples/ Representative Organisations | Reached by |
|---|---|---|
| Space Agencies, Organisations of space agencies | • Committee of Earth Observation Satellites (CEOS)<br>• Agenzia Spaziale Italiana (ASI), Italy<br>• Canadian Space Agency (CSA), Canada<br>• Center for the Development of Industrial Technology (CDTI), Spain<br>• Centre National d'Etudes Spatiales (CNES), France<br>• Comisión Nacional de Actividades Espaciales (CONAE), Argentina<br>• Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia<br>• Deutsches Zentrum für Luft-und Raumfahrt (DLR), Germany<br>• European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT), Germany<br>• European Space Agency (ESA), Europe<br>• European GNSS Agency (GSA), Europe<br>• Instituto Nacional de Pesquisas Espaciais (INPE), Brazil<br>• Aerospace Exploration Agency/Ministry of Education, Culture, Sports, Science, and Technology (JAXA/MEXT), Japan<br>• National Aeronautics & Space Administration (NASA), USA<br>• National Oceanic and Atmospheric Administration (NOAA), USA | SPACEAPPS<br>SERCO<br>FMI<br>NOA<br>CS<br>DEIMOS<br>DES<br>RESIL |

| | | |
|---|---|---|
| | • National Space Agency of Ukraine (NSAU), Ukraine<br>• Netherlands Space Office (NSO), Netherlands<br>• United Arab Emirates Space Agency (UAE SA), United Arab Emirates<br>• United Kingdom Space Agency (UKSA), United Kingdom<br>• Global Climate Observing System (GCOS), Switzerland<br>• Swedish National Space Agency (SNSA), Sweden | |
| Commercial operators of Satellite Ground Segments | • Airbus DS Geo, France<br>• Telespazio, Italy<br>• Collecte Localisation Satellites (CLS), France<br>• Planet, USA<br>• Digital Globe, (MAXAR) USA<br>• GeoEye, USA<br>• ATOS, Spain | CERTH<br>SERCO<br>SPACEAPPS |
| Commercial operators of telecommunication Satellite Ground Segments | • SES, Luxembourg<br>• Intelsat, Luxembourg<br>• Eutelsat, France<br>• Avantiplc, UK<br>• Inmarsat, UK<br>• Kongsberg Satellite Services (KSAT), Norway<br>• Hellas Sat, Greece<br>• Swedish Space Corporation (SSC), Sweden,<br>• Hispasat, Spain | SERCO<br>DEIMOS<br>DES<br>NOA<br>ENG<br>EETT |
| National and Regional Meteorological Institutes | • European Centre for Medium-Range Weather Forecasts (ECMWF), Europe<br>• Finnish Meteorological Institute (FMI), Finland<br>• Météo-France, France<br>• Institut Royal Météorologique (IRM), Belgium<br>• The Royal Netherlands Meteorological Institute (KNMI), Netherlands<br>• Instituto Portugues do Mar e da Atmosfera (IPMA), Portugal<br>• Meteorologisk Institutt, Norway<br>• Deutscher Wetterdienst, Germany<br>• Hellenic National Meteorological Service, Greece<br>• Ufficio Generale Spazio Aereo e Meteorologia, Italy<br>• Agencia Estatal de Meteorología (AEMET), Spain<br>• Swedish Meteorological and Hydrological Institute, Sweden | FMI<br>NOA<br>DEIMOS<br>DES<br>SERCO |

| | | |
|---|---|---|
| | • Met Office, UK<br>• MétéoSuisse, Switzerland | |
| EO platform operators | • SERCO, Italy<br>• Airbus Defence & Space, France<br>• Creotech Instruments, Poland<br>• Atos, France<br>• E-Geos, Italy | CERTH<br>NOA<br>SERCO<br>DEIMOS<br>DES<br>SPACEAPPS |
| Manufacturers of systems for Satellite Ground Segment | • GMV<br>• RHEA group<br>• TERMA<br>• A more complete list can be found here: https://spaceindustrydatabase.com/ | CERTH<br>NOA<br>SERCO<br>DEIMOS<br>DES<br>SPACEAPPS |

*Table 2-1 7SHIELD primary target audiences*

### 2.2.2. Secondary target audiences

| Target Group | Examples/ Representative Organisations | Reached by |
|---|---|---|
| European Association of Remote Sensing Companies (EARSC) | • Airbus, France<br>• ALPHA Consult, Italy<br>• Ariespace, Italy<br>• EOAnalytics, Ireland<br>• European Space Imaging, Germany<br>• Geospatial Enabling Technologies, Greece<br>• HISDESAT, Spain<br>• ICEYE, Finland<br>• Kongsberg Spacetec, Norway<br>• Neuropublic, Greece<br>• Planet Germany, Germany<br>• Planetek Hellas, Greece<br>• SpaceSeed, France<br>• SuperVision Earth, Germany<br>• Thales Alenia Space, France<br>• Draxis SA, Greece | CERTH<br>NOA<br>SERCO<br>DEIMOS<br>DES<br>SPACEAPPS |
| Civil Protection Agencies / Governmental Bodies | • General Secretariat for Civil Protection, Greece<br>• Dipartimento della Protezione Civile, Italy<br>• Directorate General of Civil Protection and Emergencies, Spain<br>• Civil Defence, Ministry of Interior, Cyprus | KEMEA<br>EETT<br>HP<br>RG<br>ACCELI<br>CENTRIC |

| | | |
|---|---|---|
| CI Operators, Ministries & CI Protection Agencies | • Finnish Transport Infrastructure Agency, Finland<br>• Ministry of Infrastructure and Water Management, Netherlands<br>• National Infrastructure Commission, UK<br>• Swiss Civil Protection<br>• Water Board of Nicosia, CY | KEMEA<br>ENG<br>HP<br>EETT<br>ACCELI<br>STWS |
| Cybersecurity Agencies | • European Union Agency for Cybersecurity (ENISA)<br>• European Cyber Security Organisation: ECSO<br>• European Organisation for Security (EOS) | CLS<br>CS<br>CSNov<br>KEMEA<br>HP<br>ACCELI<br>RESIL<br>RG<br>SERCO<br>CeRICT<br>INOV |
| Defence Agencies | • European Defence Agency (EDA) | ENG |

*Table 2-2 7SHIELD secondary target audiences*

## 2.3. Key communication messages

The key messages (Table 2-3) will be tailored according to the target audiences and will aim to communicate the project's objectives, its key results, and the needs it addresses.

| Target Audience | Key Messages |
|---|---|
| Space Agencies and Organisations of space agencies | • Seamless access to satellite data to serve national and global initiatives, e.g., for Disaster Risk Reduction and Climate Change monitoring. |
| Commercial operators of Satellite Ground Segments | • Shield operations through tech-driven support throughout the entire disaster/threat cycle. |
| Manufacturers of systems for Satellite Ground Segments | • Technologies that can increase their value proposition in the manufacturing of Satellite Ground Stations. |
| Group of Earth Observations (GEO) | • Safeguard satellite data and products quality and robustness. |
| European Association of Remote Sensing Companies (EARSC) | • Secure EO products access to market, and the operations of EO value chains. |
| Civil Protection Agencies / Governmental Bodies | • Provide prompt response to dangerous events and assistance in developing emergency response plans. |
| CI Operators, Ministries & CI Protection Agencies | • Ease everyday operation with the introduction of more effective protocols and processes regarding physical and cyber-attacks.<br>• Secure business continuity. |

| | |
|---|---|
| Cybersecurity Agencies | • Provision of combined and integrated new solutions for cybersecurity and assistance in decision making. |
| Defence Agencies | • Provision of early detection systems with the addition of face recognition technologies etc to monitor, detect and prevent criminal activity. |
| General Public | • Timely detection and response to emergency situations and awareness raising |

*Table 2-3 Key communication messages*

## 2.4. Roles & responsibilities

### 2.4.1. Communication Manager

The **Communication Manager (CM)** will be responsible for the coordination of the project's collaboration, clustering and networking activities. These include the infodays, project meetings, technical forums/workshops and conferences that will be organised for the dissemination of project results, as well as the relevant third-party events where the project partners will participate representing 7SHIELD.

The partner appointed by the Coordinator as the 7SHIELD Communication Manager is SERCO.

### 2.4.2. Project Communication Team

A **Project Communication Team** (PCT) has been formed, involving representatives from all project partners, to ensure the commitment to the plan and the consistency, frequency and strength of the communication actions. Each partner has designated a PCT member as follows (Table 2-4).

| Partner | PCT Member | e-mail |
|---|---|---|
| ENG | Emilia Gugliandolo | emilia.gugliandolo@eng.it |
| CERTH | Gerasimos Antzoulatos | gantzoulatos@iti.gr |
| SPACEAPPS | Leslie Gale | leslie.Gale@spaceapplications.com |
| CENTRIC | Helen Gibson | h.gibson@shu.ac.uk |
| SERCO | Franck Ranera | franck.Ranera@serco.com |
| FMI | Timo Ryyppö | timo.ryyppo@fmi.fi |
| NOA | Souzana Touloumtzi | stouloumtzi@noa.gr |
| INOV | Paulo Chaves | paulo.chaves@inov.pt |
| STWS | Katerina Kadena | k.kadena@satways.net |
| CS | Xavier Pothrat | xavier.pothrat@csgroup.eu |
| DEIMOS | Sandra Negrin | sandra.negrin@deimos-space.com |
| DES | Valeria Sulliotti | valeria.sulliotti@deimos-space.com |
| DFSL | Vinod Ahuja | vinod.ahuja@smartsecsystems.com |
| RG | John Zeppos | john.zeppos@resilienceguard.ch |

| | | |
|---|---|---|
| EETT | Vassilis Milas | vmilas@eett.gr |
| KEMEA | Agathi Barbaki | a.barbaki@kemea-research.gr |
| ACCELI | Giannis Spyropoulos | giannis.spyropoulos@accelligence.tech |
| RESIL | Francesco Brancati | francesco.brancati@resiltech.com |
| HP | Panagiotis Nikolaidis | ps.nikolaidis@astynomia.gr |
| CeRICT | Luigi Coppolino | luigi.coppolino@uniparthenope.it |
| CLS | Preetika Srivastave | preetika.srivastava@cyberlens.eu |
| CSNov | Gilles Lehmann | Gilles.Lehmann@c-s.fr |

*Table 2-4 Project Communication Team*

# 3. Communication Plan

## 3.1. Online communication channels

The online promotion of the project and dissemination of its results will be done via two main channels: a) the 7SHIELD website, and b) the 7SHIELD LinkedIn page.

To maximise the project's visibility and increase traffic on its channels, all partners will also publish information about 7SHIELD and its outputs on their organisations' websites. The partners should provide a short description of the project, the partnership, objectives and expected results, and highlight the financial support from the European Union. The information about the project has to include the programme logo with the supporting text, and links to the 7SHIELD website and LinkedIn page.

### *3.1.1. 7SHIELD Website*

The 7SHIELD website (https://www.7shield.eu/) – developed by CS and released in M3 (October 2020) – will serve as the main source of up-to-date information about the activities and outputs of the project. It will be updated by CS at least twice per month with input by all project partners and its traffic will be monitored using Google Analytics.

The website's structure, content and strategy are described with details in the deliverable *D8.3 Project Website*.

### *3.1.2. Social Media*

Because of the sensitive information related to the project, the specificity of 7SHIELD's stakeholders and its Business-to-Business orientation, LinkedIn will be the only social media platform used to relay information about the project and its results.

7SHIELD LinkedIn page (https://www.linkedin.com/company/7shield/) (Figure 3-1) has been set up and will be maintained by CS with regular input by all partners. It will be used as the project's primary online networking tool, to connect with sector-specific professional audiences, especially in the space industry, earth observation, remote sensing, critical infrastructure, security, crisis management, academia, researchers and policy-makers.

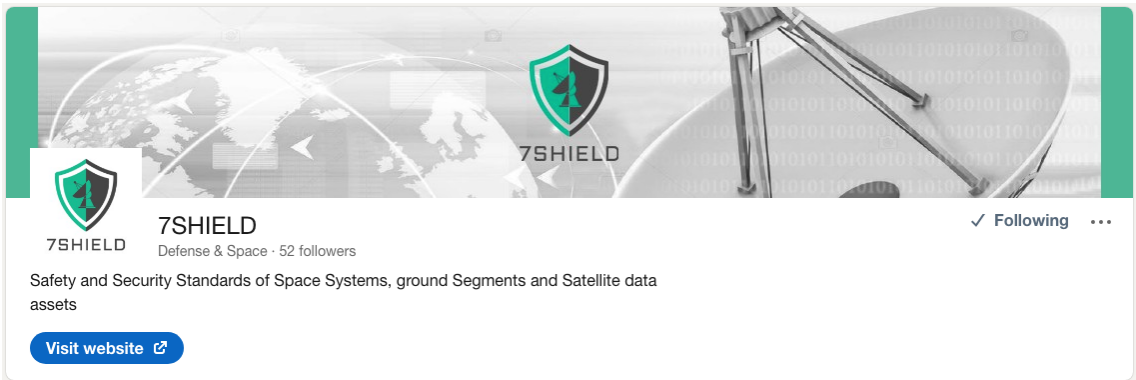


*Figure 3-1 7SHIELD LinkedIn page*

The members of the Project Communication Team will be responsible for providing content and suggestions for posts at least twice per month and CS will be in charge of managing the page and posting the approved articles on time.

To reach the widest possible audience, the partners are encouraged to like, comment, and share all activity with the appropriate audiences, through their institutional pages as well as through individual profiles.

## 3.2. Communication materials

### *3.2.1. Corporate identity*

A corporate identity has been created to support dissemination and communication activities (both internal and external) by easing information sharing and increasing 7SHIELD visibility toward its different targeted audiences.

It includes the project's logo, a graphical charter, a text document layout and a presentation layout.

The corporate identity is described with details in the deliverable *D8.2 Corporate identity and logo*.

### *3.2.2. Brochure*

Two versions of the 7SHIELD brochure will be designed by CS; the first version will be delivered in M6 (February 2021) and the final version in M24 (August 2022). The brochures will present the benefits and expected impact of the project to the general public with easy to read content for non-specialist audiences, featuring also brief information about the 7SHIELD Key Results and progress of activities.

### *3.2.3. Infoboard*

Two versions of the 7SHIELD infoboard will be designed by CS; the first version will be delivered in M6 (February 2021) and the final version in M24 (August 2022), together with the project brochures. Similarly, with the brochure, the infoboard will highlight the benefits, impact, and Key Results of the project and will be displayed at events organised by the consortium and at third-party events where 7SHIELD will be presented.

### *3.2.4. Newsletter*

An electronic newsletter will be published annually (M12 and M24), covering the latest updates of the project, addressing the general research community, as well as the primary and secondary target audiences that have been defined in Chapter 2.

The newsletter layout will be designed by CS and the Project Communication Team will provide input for the articles.

### *3.2.5. Video*

In M24 (August 2022), CS will produce a short project video to present 7SHIELD, its objectives and findings to the partners' stakeholders. The project video will be displayed in

events where 7SHIELD will be presented and will also be available online on the project website and LinkedIn page.

## 3.3. Press releases

The partners will issue press releases once per year in their countries, to communicate the most important project results, especially following the achievement of milestones (e.g. the successful pilot demonstration of 7SHIELD on a Ground Segment).

12 press releases – corresponding to the 12 countries of the consortium – are expected to be issued in the first project year (M12 – August 2021) and 12 press releases in the second project year (M24 – August 2022).

## 3.4. Content & frequency of communication activities

Communication actions will take place at least once per month and on the following indicative occasions:

- Project kick-off and organisation of kick-off meeting
- Organisation of other consortium meetings
- Organisation of workshops and infodays
- Participation of partners in third-party events
- Delivery of public reports
- Delivery of Key Results
- Pilot demonstrations of 7SHIELD
- Peer-reviewed and published scientific papers.

### *3.4.1. Social media content*

Through the 7SHIELD LinkedIn page, the partners will share information about the project results and developed technologies, peer-reviewed and published scientific publications, announcements of workshops, events, conferences, project meetings, and their respective outcomes, and also the five pilot demonstrations on the Ground Segments.

The posts will include appropriate tags and hashtags to ensure the content will reach the widest possible audiences. All institutional LinkedIn pages of the project partners should also be tagged in the posts.

Relevant hashtags for 7SHIELD include: #H2020, #cybersecurity, #space, #defence, #criticalinfrastructure, #security, #satellitedata, #satellitesystems.

### *3.4.2. Content validation process*

All communication content will be validated with the following process:

1. CS will be responsible to collect input from the Project Communication Team and build the articles and posts.

2. CS will submit the articles and posts for approval to the Project Coordinator, the Scientific and Technical Manager, the Project Security Officer, Work Package Leaders and Work Package 8 Task Leaders.
3. The content will be validated and approved within 48 hours and CS will upload it on the 7SHIELD website and LinkedIn page.

# 4. Dissemination Plan

In alignment with the Horizon 2020 guidelines, dissemination will focus on project results and will be happening only once results are available, as distinct from communication, which starts at the outset of the project to promote it as a whole.

Through the dissemination activities – which include networking events and workshops, synergies with similar H2020 projects and other initiatives, and publications – the partners will target specialist audiences identified as key stakeholders of 7SHIELD, with the aim to enable the take-up and use of results. The consortium's communication channels will also be used for dissemination.

## 4.1. Project outputs to be disseminated

| Title | Type of output | Dissemination channels |
|---|---|---|
| D2.3 Preliminary ethics and legal framework | Report | 7SHIELD Website |
| D2.6 Final ethics and legal framework | Report | 7SHIELD Website |
| D4.1 Video surveillance techniques: Initial release | Report | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D4.3 Data collection from UAVs and processing at the edge techniques | Report | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D4.5 Video surveillance techniques: Final release | Demonstrator | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D5.1 The 7SHIELD ontology and data representation model | Report | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D5.3 Security Risk Assessment Algorithms | Report | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D5.4 Social Awareness and message generation | Report | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D7.2 User training | Report | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D7.3 Field demonstrations and final system evaluation | Demonstrator | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D8.1 Communication and dissemination plan | Report | 7SHIELD Website |
| D8.2 Corporate identity and logo | Report | 7SHIELD Website |

| | | |
|---|---|---|
| D8.3 Project Website | Website | 7SHIELD LinkedIn, Partners' institutional websites, partners' institutional LinkedIn accounts |
| D8.4 Market Analysis Report v1 | Report | 7SHIELD Website |
| D8.5 Brochure and Infoboard | Report | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D8.7 Market Analysis Report v2 | Report | 7SHIELD Website |
| D8.10 7SHIELD Video | Demonstrator | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D8.12 7SHIELD Security Standardisation Strategy and policy-planning | Report | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |
| D8.13 Final brochure and InfoBoard | Report | 7SHIELD Website, 7SHIELD LinkedIn, Workshops, Infoday, Conferences |

*Table 4-1 Project outputs to be disseminated*

## 4.2. Key stakeholders

| Category | Stakeholder | Country | Interest in 7SHIELD/ contribution to tasks | Partner(s) |
|---|---|---|---|---|
| First Responders | Centre for Security Studies (KEMEA) | Greece | Project Partner & first responder in case of cyber-physical attack to NOA Ground Segment.<br>Co-design of pilot use case scenarios. | NOA |
| First Responders | Hellenic Police (HP) | Greece | Project Partner & first responder in case of cyber-physical attack to NOA Ground Segment.<br>Co-design of pilot use case scenarios. | NOA |
| First Responders | Hellenic Telecommunications and Post Commission (EETT) | Greece | Project Partner & first responder in case of cyber-physical attack to NOA Ground Segment.<br>Co-design of pilot use case scenarios. | NOA |
| First Responders | Hellenic Fire Service | Greece | National agency of Greece for fire and rescue service. First | NOA |

| | | | | |
|---|---|---|---|---|
| | | | responder in case of physical attack to NOA Ground Segment. | |
| Critical Infrastructure Owners | Greek Research & Technology Network (GRNET) | Greece | Coordinates all e-infrastructures in Education and Research in Greece. Owns the data center of NOA's Ground Segment. | NOA |
| CI Operators, Ministries & CI Protection Agencies | Centre for the Protection of National Critical Infrastructure (CPNI) | United Kingdom | Potential dissemination target group | CENTRIC |
| Civil Protection Agencies / Governmental Bodies | JESIP (Joint Emergency Services Interoperability Principles) | United Kingdom | Potential dissemination target group | CENTRIC |
| Critical Infrastructure Owners | Finnish Meteorological Institute (FMI) | Finland | Project partner and owner of the Sodankylä ground station.<br>Pilot owner | FMI |
| Technology Developer | Dr. Frucht Systems Ltd | Israel | Develop Perimeter Laser Sensor (PLS), Laser Fence Sensor (LFS), 3D Mini Drone Detector (3D MND) and Flying Hunter (FH) | DFSL |
| First Responders | Dr. Frucht Systems Ltd | Israel | Neutralisation of intruder drones | DFSL |
| First Responders | Air Zermatt | Switzerland | Search and Rescue first responders mainly for mountain operations | RG |
| Critical Infrastructure Owners | Federal Office for Civil Protection (FOCP) | Switzerland | National Risk Analysis and Reserch Coordination Body | RG |
| Critical Infrastructure Owners | OTE | Greece | Potential participation in project's dissemination activities<br>Potential contribution in Task 2.2. Stakeholder engagement user requirements | EETT |

| | | | | |
|---|---|---|---|---|
| Critical Infrastructure Owners | HELLAS sat | Greece | Potential participation in project's dissemination activities<br>Potential contribution in Task 2.2. Stakeholder engagement user requirements | EETT |
| Critical Infrastructure Owners | Forthnet | Greece | Potential participation in project's dissemination activities<br>Potential contribution in Task 2.2. Stakeholder engagement user requirements | EETT |
| Critical Infrastructure Owner | Ice Cubes ground Segment | Belgium | Ice Cubes facility operation onboard the International Space Station. User access to experiments in the facility | SPACEAPPS |

*Table 4-2 7SHIELD Key Stakeholders*

## 4.3. Networking activities

The networking activities aim to create and maintain links, both between the project partners but also with the external communities involved in the context of 7SHIELD. Participation to events and communication with other initiatives are used to develop and strengthen the relations. Publications are used for raising awareness and to ensure a regular communication. Network activities organized proactively including:

- Internal Workshops and progress meetings to keep all partners connected and informed on feedback received from external events (Third Party). Internal events give partners the necessary material to communicate externally project progress and pilot results as well as share the 7SHIELD vision on how the community is evolving and which are the technologies commonly used or innovations requested.
- Third party events like International conferences and participation to synergize with other H2020 projects promoting 7SHIELD towards relevant communities. Third Party events allow to promote the internal works and make contacts to experts and recognized professionals who will be involved in the project InfoDays ("European Project Workshop" foreseen in April 2022).

Any communication made within the context of these events respects the security constraints of the project.

### 4.3.1. Project events & workshops

A particular attention is brought on the communication around the events listed below. Each event will be clearly reported, and relevant information will be shared internally to the project partners, using the communication channels described in Chapter 3 and material described in Chapter 4.

The European Project Workshop will be prepared, starting today with a clear plan, emphasizing the critical items and the Key characteristics for each of the following categories:

- Construction of Participants' list
- Setup of the Agenda
- Selection of event location (physical or virtual)
- Marketing and communication material
- Shipment of Invitation
- Set up of the event.

Table 4-3 lists the internal events identified to develop the networking activities.

| Name of event/ workshop | Location | Scope | Organiser | Participants |
|---|---|---|---|---|
| European Project workshop | To bet setup according to COVID-19 situation | Share results and lessons learnt to stakeholders.<br>Disseminate project results and success stories to all categories of the target audiences. | WP8 T8.2 | All relevant partners |
| Pilot Infoday | Meeting at Pilot leaders' premises | Raise awareness on Pilot status.<br>Present results. | Pilot leaders | All relevant partners |
| Project Progress Meetings | Virtual Meeting | Communicate on project progress.<br>Share messages from Third Party event.<br>Identify issues and decide on actions. | WP leaders | Relevant WP |
| GEO side event | To bet setup according to COVID-19 situation | Advocate the importance of 7SHIELD for enhancing the resilience of Space Ground Segments. | WP8 T8.2 | Relevant WP leaders |

*Table 4-3 7SHIELD events & workshops*

### 4.3.2. Participation in third-party events

To boost the networking activities with third parties, each partner will contribute by:

- Communicating and participating to at least two international events where the promotion of 7SHIELD is extremely valuable. We will list international conferences, starting with EC and ESA organized events, where a generic presentation of the project will be held. We are also looking for specialised workshops to emphasise a specific asset of 7SHIELD and develop the network with targeted stakeholders (for example the security authorities). The recognised experience and the network established by each partner is exploited here. It aims to bring the right message to the right audience.
- Providing feedback on the outcomes of the conferences following an established procedure. This "Conference Report" process is under finalisation, but headlines emphasise the following points:
  - Conference details (title, date)
  - Audience (remote sensing, detection, IoT, semantics, security…)
  - Contribution details (abstract and presentation)
  - Article to be published through 7SHIELD communication channels (web portal, news, social networks)
  - Network established (PoC of key persons, recognize stakeholders).

The third-party event list is already shared among the partners and first contributions have been received demonstrating that partners embrace the effort. The table is an internal dynamic tool and will be maintained up to date when events pop up. The final decision to participate is to be taken at WP / Project Management level but it structures the communication and networking strategy of the project.

In addition, the project maintains its proactive approach via synergies with other projects dealing with securing critical infrastructure. One example is the European Cluster for Securing Critical infrastructures (ECSCI) that 7SHIELD will join to share its outcomes and benefits from the experience from projects that present synergies.

Table 4-4 provides an indicative subset of the information collected so far for Third Party Events. The internal events monitoring table, together with the Conference Report will help generating reports focusing on KPIs listed in the Grant Agreement.

| Name of event | Number of Attendees | Location | URL |
|---|---|---|---|
| Phi Week (side event) | 20+ | Virtual | https://phiweek.esa.int/ |
| Nicosia Risk Forum 2020 | 50+ | Virtual | https://cerides.euc.ac.cy/nicosia-risk-forum/nicosia-risk-forum-2020/ |
| International conference on natural hazard and | 50+ | Athens, Greece | https://iconhic.com/2021/ |

| | | | |
|---|---|---|---|
| infrastructure (ICONHIC) 2021: THE STEP FORWARD | | | |
| International Conference on Sustainable Industrial Development | 50+ | Istanbul, Turkey | https://waset.org/sustainable-industrial-development-conference-in-february-2021-in-istanbul |
| International Conference on Space Technologies | 50+ | Toronto, Canada | https://waset.org/space-technologies-conference-in-july-2021-in-toronto |
| CIPRE-EXPO | 20+ | Bucharest, Romania | https://www.cipre-expo.com/ |
| ESREL | 20+ | Angers, France | http://esrel2021.org/en/index.html |
| ESORICS | 20+ | Darmstadt, Germany | https://esorics2021.athene-center.de/ |
| International Conference on Critical Infrastructure Security (CRITIS2021) | 50+ | Lausanne, Switzerland | https://critis2021.org/ |
| International Conference on Information Systems for Crisis Response and Management (ISCRAM2021) | 50+ | Blacksburg, Virginia, USA | https://www.drrm.fralinlifesci.vt.edu/iscram2021 |
| 8th European Ground System Architecture Workshop | 20+ | Virtual (TBD) | |
| Ground System Architecture Workshop | 20+ | Virtual | https://gsaw.org/ |

*Table 4-4 Third-party events*

### *4.3.3. COVID-19 and health considerations*

The COVID-19 pandemic has a strong impact on the dissemination activities of EU-funded projects, including those of 7SHIELD. The Project Coordinator and the Project Management Board will closely monitor the precautionary and mitigation measures enforced by the governmental authorities of the partnership countries and decide about the format of the foreseen workshops and networking events accordingly.

During lockdown periods, the partners will opt for virtual events instead of physical ones, on condition that the scope and content of the events is not substantially affected. In case the scope is severely affected by the restrictive measures and the event or workshop cannot take place virtually, the Project Coordinator will promptly contact the Project Officer, to explore alternative options and implementation of the force majeure clause of Article 51 of the H2020 Annotated Model Grant Agreement.

## 4.4. Synergies with relevant research & innovation activities

| Project Title | Relevance to 7SHIELD | Responsible Partner(s) |
|---|---|---|
| H2020 SAFECARE | Focusing on health services infrastructure, SAFECARE develops threat prevention, detection, response and mitigation of impacts across CI, populations and environments and delivers an innovative decision support system. | KEMEA |
| H2020 InfraStress | InfraStress addresses the cyber-physical security of Sensitive Industrial Plants and Sites (SIPS) Critical Infrastructures and improves the resilience and protection capabilities of SIPS exposed to large scale, combined C/P threats and hazards, guaranteeing continuity of operations while minimising cascading effects. 7SHIELD will benefit from the integrated C/P Situational Awareness and C/P Threat Intelligence developed in InfraStress. | ENG<br>INOV<br>STWS<br>CERTH |
| H2020 SecureGas | SecureGas focuses on the 140.000Km of the European Gas network covering the entire value chain from Production to Distribution to the users, providing methodologies, tools and guidelines to secure existing and incoming installations and make them resilient to cyber-physical threats. | KEMEA |
| H2020 SATIE | SATIE adopts a holistic approach about threat prevention, detection, response and mitigation in the airports, while guaranteeing the protection of critical systems, sensitive data and passengers. | KEMEA<br>INOV<br>STWS |
| H2020 DEFENDER | DEFENDER aims to model Critical Energy Infrastructures (CEIs) as distributed Cyber-Physical Systems for managing the potential reciprocal effects of cyber and physical threats deploying intrusion detection and UAV neutralisation solutions. | DFSL<br>ENG |
| H2020 Net2DG | Leveraging Networked Data for the Digital electricity Grid. Deployment of methodologies for threat assessment and anomaly detections solutions for faults and attacks. | RESIL |
| ESA – Sentinels Rolling Archive User Access, Operations, Maintenance | Engagement with ESA to define the new requirements of the Sentinel rolling archive access mechanism and incorporate 7SHIELD technologies in the Payload Data Ground Segments (PDGS) to increase resilience and ensure service continuity in case of cyber and physical attacks. | NOA<br>SERCO<br>GAEL |
| SECEF | The aim of the SECEF (SECurity Exchange Format) project is to promote and improve the use of open standard in cyber-security. | CSNov |
| H2020 EU-CIRCLE | EU-CIRCLE is a pan-European framework for strengthening Critical Infrastructure resilience to climate change. 7SHIELD will capitalise on the Climate Infrastructure Resilience | STWS |

| | | |
|---|---|---|
| | Platform developments that will be tested for satellite ground stations infrastructure. | |
| H2020 SafeShore | System for detection of Threat Agents in Maritime Border Environment | DFSL |
| SCAAN | Security Communications and Analysis Network. SCAAN is a project and service run by CENTRIC and the International Organisation for Migration that supports crisis communications with staff members during major security incidents. 7SHIELD will inform and be informed by SCAAN 's work on best practice crisis communications and social awareness. | CENTRIC |
| HYPERION | Hyperion aims at providing a system that will facilitate and support Cultural Heritage sites Resilience along with the local community and business ecosystem, against natural hazards and climate change | RG |
| ECSCI Cluster | European Cluster for Securing Critical Infrastructures - ECSCI is a cluster of H2020 projects for securing critical infrastructures whose main objective is to bring about synergetic, emerging disruptive solutions to security issues via cross-projects collaboration and innovation. | ENG<br>INOV |
| CIP PROTECTION - Targeted Actions for enhancing the protection of National Characterized European Critical Infrastructure – NCECI | The project "Targeted Actions for enhancing the protection of National Characterized European Critical Infrastructure – NCECI", includes a series of actions and deliverables that are being developed in order to provide the background for a commonly acceptable level of safety and protection for the NCECI. To this end, it is critical to ensure the systematic cooperation of the bodies that are responsible for the safety and protection of citizens with the operators and in particular the Security Managers of the Infrastructures. Its main goal is to define a framework of synergies between those involved in security, protection and the sound operation of infrastructures that will contribute to the strengthening of the resilience of society, for the smooth operation of which, critical infrastructure constitute a key pillar. | KEMEA |

*Table 4-5 Synergies with other projects*

## 4.5. Publications

The project foresees at least 15 scientific or academic open access publications in technical and scientific conferences and journals, and in industry-led magazines and websites.

**Relevant journals include:**

- International Journal of Protective Structures
- International Journal of Information Security
- International Journal of Critical Infrastructure Protection

- IEEE Transactions on Dependable and Secure Computing
- Security Journal
- IEEE Transactions on Geoscience and Remote Sensing
- International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences (ISPRS Archives).

Relevant general security conferences include:

- Cyber Security for Critical Assets Europe (CS4CA)
- International Conference on Critical Information Infrastructures Security (CRITIS)
- Critical Infrastructure Protection & Resilience Europe
- International Conference on Information Systems for Crisis Response and Management (ISCRAM)
- International Symposium on Research in Attacks, Intrusions and Defences (RAID)
- European Safety and Reliability Conference (ESREL)
- BlackHat Europe
- CRESTCon - The technical cyber security industry conference
- IFIP Information Security Conference & Privacy Conference
- IFIP Technical Committee 11
- IFIP Working Group 11.10 on Critical Infrastructure Protection
- International Defence and Homeland Security Simulation Workshop (DHSS)
- Risk-In 2020, Annual Conference for Risk and Resilience matters.

Relevant space sector conferences include:

- International Conference on Natural Hazards & Infrastructure (ICONHIC)
- International Conference on Sustainable Infrastructural Development (ICSID)
- European Safety and Reliability Conference (ESRC)
- ESA Living Planet Symposium (LPS)
- ESA EO Phi-Week
- Toulouse Space Show (TSS)
- PSSI Space Security Conference
- ISDE International Symposium on Digital Earth
- Big Data from Space
- IEEE Geoscience and Remote Sensing Society
- European Geosciences Union General Assembly
- International Geoscience and Remote Sensing Symposium - IGARSS 2021 (https://www.igarss2021.com/default.asp)

Relevant multimedia conferences include:

- International Conference on Multimedia Modeling (MMM)
- ACM International Conference on Multimedia
- Annual ACM International Conference on Multimedia Retrieval (ICMR)
- Conference on Computer Vision and Pattern Recognition (CVPR).

# 5. Impact and performance

## 5.1. Key Performance Indicators

The success of the communication and dissemination actions will be evaluated throughout the project duration based on specific metrics, outlined in Table 5-1.

| Tool | KPIs | Target value(s) |
|---|---|---|
| 7SHIELD Website | Number of visits | 10000 |
| | Number of downloads of public outputs | 300 |
| 7SHIELD LinkedIn | Number of page followers | 300 |
| | Number of monthly posts | 2-3 |
| | Number of views per post | 100 |
| | Number of reactions per post | 50 |
| | Number of shares per post | 10 |
| Brochure | Number of brochures printed and distributed to the target audiences | 500 |
| Infoboard | Number of infoboards displayed at events | 10 |
| 7SHIELD Video | Number of views | 100 |
| Newsletter | Number of newsletters issued | 2 |
| | Number of subscribers | 300 |
| Publications | Number of publications in technical and scientific conferences and journals, and industry-led magazines and websites | 15 |
| Workshops | Number of organised workshops | 4 |
| | Number of participants per workshop | 50 |
| 7SHIELD Infoday | Number of participants | 200 |
| Press releases | Number of press releases distributed to local, national and European media | 24 |

*Table 5-1 Key Performance Indicators*

## 5.2. Monitoring and reporting

The implementation of communication and dissemination actions will be systematically monitored throughout the project duration. An internal monitoring tool (i.e. an online form) will be created by NOA to assist the reporting process. All partners will report every communication activity they perform on the tool, providing specific information that will be requested (e.g. description of action, communication channel, target audiences, number of individuals reached). Information on the success of the 7SHIELD website and LinkedIn page will be provided by CS – the partner responsible for the management of the project's online communication channels.

The performance of the communication and dissemination actions will be officially reported in the deliverables *D8.8 – Final report on communication and dissemination activities* (to be delivered by CS in M23) and *D8.9 – Final networking report* (to be delivered by SERCO in M23).

# 6. Compliance considerations

## 6.1. Visibility of EU funding

In compliance with Article 38 of the H2020 AMGA "Promoting the action – visibility of EU funding", all communication related to the project – including electronic communication via email, newsletters, project website and institutional websites, use of social media – and all infrastructure, equipment or results funded under the specific grant must:

- display the EU emblem

- display the supporting text next to the emblem: "This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883284".

The minimum height of the EU emblem shall be 1 cm and the name of the European Union shall be spelled out in full. The font can be Arial, Calibri, Garamond, Trebuchet, Tahoma or Verdana with no font effects, and the font size should be proportionate to the size of the emblem.

## 6.2. GDPR

All partners are obliged to comply with the GDPR legislation for all communications with other businesses and organisations and for use of third-party data, including those initiated in the context of enacting the 7SHIELD communication strategy. The 7SHIELD partnership will treat all data collected as confidential and strictly use it under the framework of the 7SHIELD project activities in compliance with the EU legal regulations. The scope of the data collected will be the minimum necessary for each purpose, avoiding as much possible personal information. No personal information will be collected without the knowledge and consent of the target audience, using the dedicated Participant Information Sheet and Participant Consent Form that have been provided by the Project Coordinator.

In D9.4 – POPD - Requirement No. 4 (due at M2), all partners are advised to contact their internal Data Protection Officer before contacting third-party organisations and individuals outside the project partnership.

## 6.3. Security considerations

The Security Advisory Board (SAB) will be an integral part of the formulation of the dissemination and communication strategy in order to act pro-actively. In this direction the following procedures will be applied:

- The whole dissemination and communication strategy of the project results to wider audiences and shall be supported by the Security Advisory Board (SAB), which shall report to the Commission (through the Coordinator) when needed;
- Before commencement of any dissemination activity (e.g., publication in scientific journal or presentation in workshop) the SAB should review the material (e.g.,

academic article or presentation) in order to avoid publication of material containing sensitive information.

# 7. Timeplan of activities & partners' involvement

| Activity | Responsible partner(s) | Deadline |
|---|---|---|
| Creation of 7SHIELD LinkedIn page | CS | 31/10/2020 |
| Announce 7SHIELD kick-off on LinkedIn page | CS | 31/10/2020 |
| Follow and share 7SHIELD LinkedIn page with own network | ALL | 15/11/2020 |
| Submission of Communication and dissemination plan | NOA | 30/11/2020 |
| Submission of Corporate identity and logo | CS | 30/11/2020 |
| Development of Project Website | CS | 30/11/2020 |
| Update project website content | CS | 30/11/2020 |
| Post introductory article about 7SHIELD on institutional websites | ALL | 30/11/2020 |
| Update project website content | CS | 31/12/2020 |
| Update project website content | CS | 31/01/2021 |
| Design of Brochure and Infoboard | CS | 28/02/2021 |
| Update project website content | CS | 28/02/2021 |
| Update project website content | CS | 31/03/2021 |
| Update project website content | CS | 30/04/2021 |
| Update project website content | CS | 31/05/2021 |
| Update project website content | CS | 30/06/2021 |
| Provide input for 1st issue of 7SHIELD newsletter | ALL | 31/07/2021 |
| Update project website content | CS | 31/07/2021 |
| Update project website content | CS | 31/08/2021 |
| Publish 1st issue of 7SHIELD newsletter | CS | 31/08/2021 |
| Update project website content | CS | 30/09/2021 |
| Update project website content | CS | 31/10/2021 |
| Update project website content | CS | 30/11/2021 |
| Update project website content | CS | 31/12/2021 |
| Update project website content | CS | 31/01/2022 |
| Update project website content | CS | 28/02/2022 |
| Update project website content | CS | 31/03/2022 |
| Update project website content | CS | 30/04/2022 |

| | | |
|---|---|---|
| Update project website content | CS | 31/05/2022 |
| Update project website content | CS | 30/06/2022 |
| Final report on communication and dissemination activities | CS | 31/07/2022 |
| Final networking report | SERCO | 31/07/2022 |
| Update project website content | CS | 31/07/2022 |
| Provide input for 2nd issue of 7SHIELD newsletter | ALL | 31/07/2022 |
| Update project website content | CS | 31/08/2022 |
| 7SHIELD Video | CS | 31/08/2022 |
| Design of Final brochure and infoboard | CS | 31/08/2022 |
| Publish 2nd issue of 7SHIELD newsletter | CS | 31/08/2022 |

*Table 7-1 Timeplan of activities*

# 8. Conclusions

The Communication and Dissemination strategy elaborated in this document aims to set the basis for maximising the visibility of the project and the uptake of its results. The plan will be considered a living and evolving document, which will be updated and enhanced as the activities of 7SHIELD progress and as more opportunities for networking, H2020 synergies and promotion of the project appear. All communication and dissemination activities will be continuously monitored by the Project Communication Team and the strategy will be fine-tuned according to the overall performance and estimated impact.


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