Ref. Ares(2022)5717606 - 12/08/2022

D10.3 Communication Strategy and Dissemination Plan v2

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 101021274

Protection of Critical Infrastructures from advanced combined cyber and physical threats

Deliverable nº:	D10.3
Deliverable name:	Communication Strategy and Dissemination Plan v2
Version:	1.0
Release date:	29/07/2022
Type* - Dissemination level**	Report - Public
Status:	Final version
Editors	ICCS
Contributing WP	WP10

Abstract

The present deliverable contains update of the Communication Strategy and Dissemination plan of the PRAETORIAN Project for the 2nd year of its running life, aiming to define the purpose of communication results, news, and other relevant information, alongside with the different dissemination channels identified under the scope of PRAETORIAN.

**Type*. Report; Demonstrator; Ethics*

***Dissemination Level*. Public; Confidential (Confidential, only for members of the consortium (including the Commission Services)); RESTREINT UE (Classified information, RESTREINT UE (Commission Decision 2015/444/EC)).*

Disclaimer

This document contains material, which is the copyright of certain PRAETORIAN beneficiaries, and may not be reproduced or copied without permission.

The information appearing in this document has been prepared in good faith and represents the views of the authors. Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authors accept no statutory, contractual or other legal liability for any error or omission to the fullest extent that liability can be limited in law.

This document reflects only the view of its authors. Neither the authors nor the Research Executive Agency nor European Commission are responsible for any use that may be made of the information it contains. The use of the content provided is at the sole risk of the user. The reader is encouraged to investigate whether professional advice is necessary in all situations.

No part of this document may be copied, reproduced, disclosed, or distributed by any means whatsoever, including electronic without the express permission of the PRAETORIAN project partners. The same applies for translation, adaptation or transformation, arrangement or reproduction by any method or procedure whatsoever.

PRAETORIAN

PRAETORIAN strategic goal is to increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats. To that end, the project will provide a multidimensional (economical, technological, policy, societal) yet installation-specific toolset comprising: (i) a Physical Situation Awareness system, (ii) a Cyber Situation Awareness system; (iii) a Hybrid Situation Awareness system, which will include digital twins of the infrastructure under protection; and (iv) a Coordinated Response system. The PRAETORIAN toolset will support the security managers of Critical Infrastructures (CI) in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

The project specifically tackles (i.e. prevent, detect, response and, in case of a declared attack, mitigate) human-made cyber and physical attacks or natural disasters affecting CIs. It also addresses how an attack or incident in a specific CI can jeopardise the normal operation of other neighbouring/interrelated CIs, and how to make all of them more resilient, by predicting cascading effects and proposing a unified response among CIs and assisting First Responder teams.

PRAETORIAN is a CI-led, user-driven project, which will demonstrate its results in three international pilot clusters, some of them cross border -Spain, France and Croatia-, involving 9 outstanding critical infrastructures: 2 international airports, 2 ports, 3 hospitals and 2 power plants.

Document history:

Version	Date of issue	Content and changes	Partner
0.1	20/06/2022	ToC	ICCS
0.6	01/07/2022	Contributions by ICCS	ICCS
0.7	20/07/2022	Review by RINI	RINI
0.8	25/07/2022	Review by Koncar	Konkar
0.9	28/07/2022	Review by EDF	EDF
1.0	29/07/2022	Final version ready for submission	EDF

List of Authors:

Partner	Author
ICCS	Konstantinos Demestichas, Konstantina Remoundou, Lazaros Papadopoulos

Peer reviewed by:

Partner	Reviewer
RINI	Jelena Ravak
Končar	Tamara Hadjina
EDF	Farina Siham
ETRA	Eva Munoz

Table of Contents

Index of Tables

Index of Figures

Abbreviations and Acronyms

CP	Consortium Plenary
DoA	Description of Action
CERIS	Community for European Research and Innovation for Security
CI	Critical Infrastructure
EC	European Commission
ECSO	European Cyber Security Organisation
ECSCI	European Cluster for Securing Critical Infrastructures
FRs	First Responders
GNU	General Public License
H2020	Horizon 2020. The EU Framework Programme for Research and Innovation
KPI	Key Performance Indicator
LEA	Law Enforcement Agency
PC	Project Coordinator
PDF	Portable Document Format
PMB	Project Management Board
PO	Project Officer
QA	Quality Assurance
SEO	Search Engine Optimization
SME	Small-Medium Enterprise
TL	Task Leader
TM	Technical Manager
TRL	Technology Readiness Level
URL	Uniform Resource Locator
WP	Work Package
WPL	Work Package Leader

Executive Summary

This deliverable is an updated version of the dissemination and communication strategy of PRAETORIAN, which was initially defined in D10.2 and submitted on M2. It describes how the dissemination strategy, which was agreed and defined during the starting phase of the project is materialized up to M14, and how this strategy was adapted and fine-tuned during the 1st year of the project.

Compared to the D10.2, this present version includes the following additional information:

- The current list of relevant project stakeholders
- A short description of the clusters in which the project participates
- A list of all past and planned dissemination activities (publications, participation in events, etc.)
- Update on dissemination KPIs
- A Crisis Communication Procedure

Finally, the main dissemination activities that have taken place during the first year of the project are the following:

- Participation in 13 conferences and workshops, including ECSCI cluster activities, as well as in 3 forums of significant visibility
- Publication of 3 newsletters and two scientific publications

The most important planned dissemination event includes the organization of the PRAETORIAN workshop with the participation of members of the Stakeholders Group and sister projects.

1. Introduction

1.1 Purpose of the document

Communication, dissemination, and exploitation are key concepts in any project and PRAETORIAN is not an exception. PRAETORIAN specifically tackles (i.e., prevent, detect, respond, and mitigate) human-made cyber and physical attacks or natural disasters affecting Critical Infrastructures (CIs).

All PRAETORIAN partners are strongly committed to exploiting the project outcomes, and further pursuing its vision, ensuring the project's long-term continuity well beyond its finish time. Dissemination, communication, and exploitation activities are three tightly connected pillars that will lead to raising the awareness of the PRAETORIAN system – relevant challenges and achievements as the project progresses, generating expectations among the targeted communities and paving the way for fertile synergies and business collaborations. Under this light, this document is an update of D10.2 "Communication Strategy and Dissemination Plan v1", which was submitted in M2.

1.2 Scope of the document

The PRAETORIAN project team devises and implements personalized strategies and communication plans to ensure they meet the motivations, attitudes, and interests of each target audience. A streamlined approach is used that produces and documents a very clear communication strategy, a detailed communication action plan and a set of associated outcomes. It is the first critical step in a process that ensures that the project consortium has a clear understanding and agreement on the overall mission for communication, key audiences / stakeholders, key communication programs / activities, key messages for each audience / stakeholder, key measures of effectiveness, as well as roles and responsibilities for communication.

The implementation of this methodology ensures that the project maximizes the impact that can be achieved across targeted audiences.

1.3 Structure of the document

To be assured that all communication is relevant to the core objectives of the agreed upon dissemination strategy and that key messages are consistently delivered the deliverable is structured by answering a set of simple questions. Ergo, Section 2 includes the dissemination plan and activities of PRAETORIAN, by answering the following questions:

- Why communicate information about PRAETORIAN?
- What does the audience need to know?
- Who/which are the key audiences?
- Where is the best "place" to reach the targeted audiences?
- When should the message be delivered to increase efficiency?
- How to deliver the most effective message?

In addition, section 2 also includes the results and progress of the actions agreed in the 1st year of the project including events the PRAETORIAN partners have attended to, publications, social media analytics etc. Finally, Section 3 summarizes all the above points and concludes on the results of the communication and dissemination activities of the first 14 project months.

2. Communication & Dissemination Plan and Activities

An important part of the project's strategy is to effectively plan communication activities and to monitor the success in reaching and engaging with stakeholders. The communication activities are structured in a coherent and integrated way to ensure high visibility and to maximize the impact of the project.

In that light, in order to maximize the impact of all communication and dissemination activities, a clear strategy is defined, and its specific objectives are identified. To ensure that the PRAETORIAN results are communicated and disseminated according to the expectations of all members of the consortium, strategic objectives for all dissemination and communication activities have been identified and are presented below. These objectives are:

- To ensure that it is clear to the target audiences that more results have been achieved than otherwise possible, as a consequence of the EU-wide collaboration in the PRAETORIAN project;
- To demonstrate how the outcomes of the PRAETORIAN project are relevant to the everyday lives of a growing cohort of European citizens. In addition, the relevance will be demonstrated through the creation of new jobs within the EU as a result of the exploitation of project results and outputs.
- To make sure, where possible, that the results of the PRAETORIAN project influence policy and decision makers in industry and the scientific community in order to ensure the long-term impact of the project.
- To ensure that all communication produced is engaging and interesting to the target audience.

2.1 General Guidelines

Due to the large set of information that should be communicated regarding the PRAETORIAN project, a set of basic rules need to be followed by each communication action. The guidelines are presented below:

- To ensure that all legal, ethical and privacy criteria are being considered and met;
- To comply with the project's procedures, scope, objectives according to contractual documents;
- To respect the Grant Agreement (GA), Description of Action (DoA) and Consortium Agreement (CA);
- To guarantee the proper use of the funding for maximum efficiency, to demonstrate value for money for all dissemination activities conducted;
- To use the official project material in presentations;
- To avoid publication of restricted and/or commercial data and to ensure that all the necessary procedures prior any publication have been followed;
- To make sure security restrictions and confidentiality are preserved (the Security Advisory Board should be consulted if required);
- To create a responsive and adequate activity addressing the appropriate target audience;

- To avoid the repeated publication of the same work;
- To avoid publication of one's work without proper referencing;
- To guarantee proper referencing and archiving of all dissemination material.

These rules serve as guidelines for all communication activities and should be verified before any outreach by the beneficiary responsible for the given outreach activity.

2.2 Why: The aim of communication and dissemination

The first question to clarify in this document is "why" PRAETORIAN wants to communicate. This question and the answers are especially important since they will drive all the following activities with a clear purpose in mind.

The multiple communication objectives are based on the strategic objectives, and they are summarized below:

- Convince the target audiences that the PRAETORIAN project is a powerful key-enabler for achieving scientific excellence, contributing to competitiveness and solving important societal challenges;
- Demonstrate how the outcomes of the PRAETORIAN project are relevant to the everyday lives of a growing cohort of European citizens by increasing the safety and resilience of our society, protecting lives, creating jobs, introducing novel technologies, or positively effecting citizens' lives in other ways;
- Where possible, make sure that the results of the PRAETORIAN project influence policy and decision makers in industry and the scientific community, in order to ensure the long-term impact of the project;
- Build synergies with other EU-funded projects, networks and initiatives, avoiding duplication and maximizing the impact.

2.3 What: Communication and dissemination content

2.3.1 Dissemination and Communication Dashboard

To ensure that all the necessary actions are being implemented during the lifetime of the project, since M2 PRAETORIAN has initialized the Dissemination and Communication Dashboard in the form of an excel file. This reporting dashboard is intended to be used by the PRAETORIAN consortium to track and record all the communication and dissemination activities undertaken by project partners during the project. It is essential for every partner to familiarize themselves with this tool and keep it updated throughout the whole project.

PRAETORIAN
Protection of critical infrastructures from advanced cyber-physical threats

Figure 1. PRAETORIAN Dashboard

2.4 Who: Relevant stakeholders

Considering the nature and objectives of PRAETORIAN, as well as the societal impact and expectations, the target audience of communication and dissemination activities is quite broad, ranging from the community of LEA officers, FRs, CI owners and operators, to policy and decision makers (city security managers, government and other public authorities), and from the research and academic community to industrial stakeholders (large companies, SMEs or dedicated experts) eager to commercially exploit the project outcomes and findings. Thus, the PRAETORIAN dissemination and communication plan ensures its effectiveness by appropriately tailoring the communicated messages and the associated communication channels according to the specific target group, suitably defining objectives and quantifiable indicators and continuously monitoring the results against these indicators, introducing amendments and adjustments if required.

The Table 1. below is the latest updated list of the PRAETORIAN Stakeholder Group.

Table 1: The PRAETORIAN Stakeholders Group

Organization Name	***Location***	***Sector***	***Type***
Police Directorate	Croatia	Government	Law Enforcement Authority
Civil Protection Directorate	Croatia	Government	Governmental Body
Valencia Local Police	Spain	Government	Law Enforcement Authority
EUROCONTROL	Belgium	Transportation / Aviation	European Organization

G4S Telematics	Greece	Transportation	Industrial Enterprise
International Union of Railways (UIC)	France	Transportation / Rail	International Organization
HOPS	Croatia	Power / TSO	CI Operator
Association Exera	France	Industrial Association	European Organization
Grand Lyon	France	Government	City Administration
Ministry of the Interior	Austria	Government	Governmental Body
Municipality of Vienna	Austria	Government	City Administration
Wiener Linien	Austria	Transportation	CI Operator
Wiener Netze	Austria	Power / TSO	CI Operator
Vienna Airport	Austria	Transportation / Aviation	CI Operator
Linz AG	Austria	Multi-Utility Provider	CI Operator
Stadtwerke Klagenfurt	Austria	Multi-Utility Provider	CI Operator
Interport Police	USA	Stakeholder Association	International Organization
Piraeus Port Authority	Greece	Transportation / Maritime	CI Operator
European Cyber Security Organisation	Belgium	Stakeholder Association	European Organization
European Organisation for Security	Belgium	Stakeholder Association	European Organization

2.5 Where: Choose appropriate channels

2.5.1 Online Presence

A dynamic and interactive website, together with social media accounts – particularly Twitter and LinkedIn – has been created and is continuously being updated and maintained to boost information flow to all entities with an interest in the project, following the guidelines set in [1]. These online means will also be used to disseminate relevant information to targeted parties. Table 2 summarizes the social media targets.

Publicly available information that is in use for this purpose includes:

- Information on the project, its objectives, its challenges and the main results and achievements;
- Information about the consortium members and all organizations involved;
- Project news (e.g., announcement of project events);
- Public deliverables of the project;
- Publications, conference proceedings and journal articles;
- Links to websites of interest to the project (complementary research, other national and European initiatives relevant to the project).

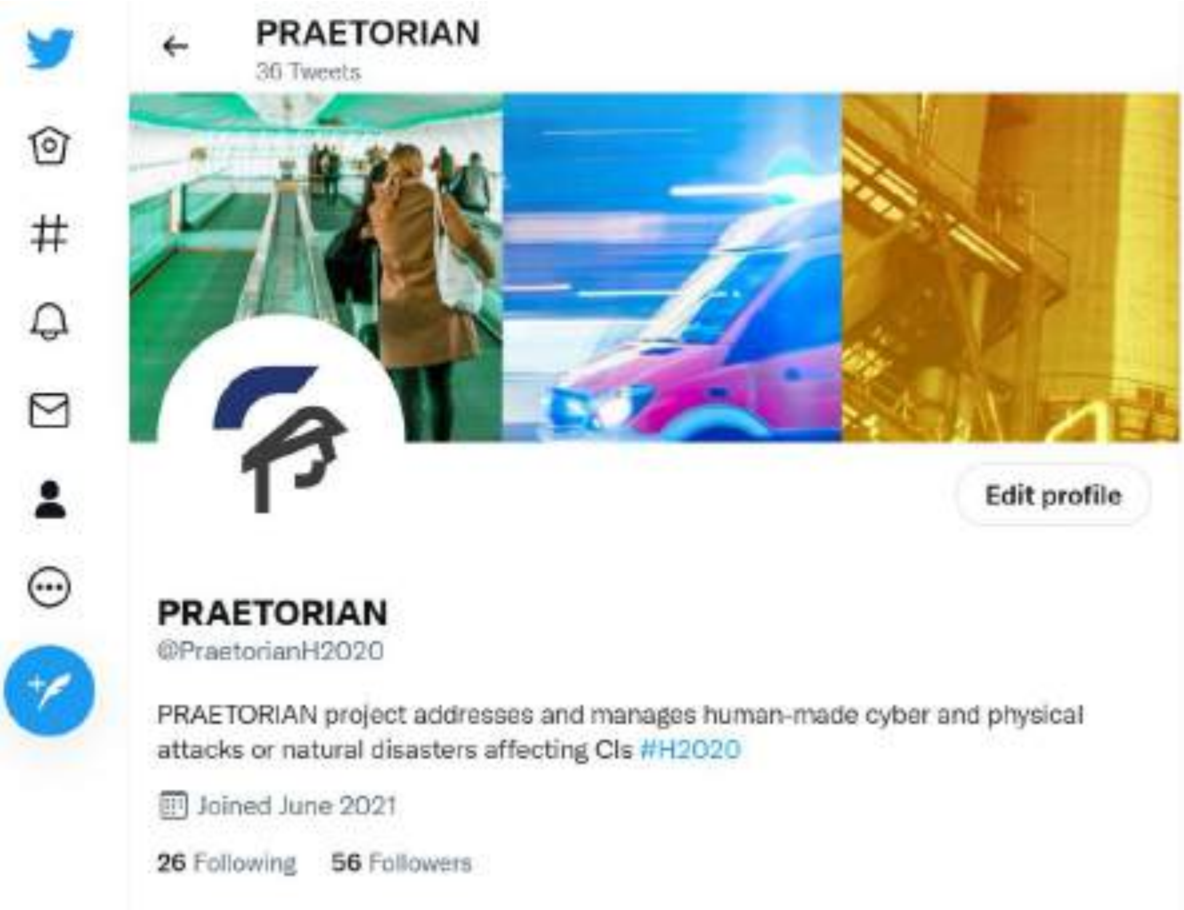
Additionally, a repository has been created for sharing internal information between the consortium partners and for archiving the project documents.

Table 2. Online communication plan

	Targeted community	**Key Performance Indicator**	**KPI Target Value**	**KPI value on the end of 1st year**	**Reach level**	**Links**
Project website	General public, local/ regional/ national authorities, EC, LEAs, industrial companies, SMEs, scientific/ research community	Number of visitors, number of returning visits, stay-on-page time, other Search Engine Optimization (SEO) metrics	1500 unique visitors	788	International	https://praetorian-h2020.eu/
LinkedIn	General public, local/ regional/ national authorities, EC, LEAs, industrial companies, SMEs, scientific/ research community	Number of subscribers	100 members	82	International	https://www.linkedin.com/company/praetorian-h2020
Twitter	General public, local/ regional/ national authorities, EC, LEAs, industrial companies, SMEs, scientific/ research community	Number of followers	150 followers	55	International	https://twitter.com/PraetorianH2020
Multimedia content	General public, local/ regional/ national	Number of videos produced	2 videos	1st video will be ready before the	International	

	authorities, EC, LEAs, industrial companies, SMEs, scientific/research community			intermediate review		
Newsletters (email)	Local/ regional/ national authorities, EC, LEAs, industrial companies, SMEs, scientific/ research community	Number of newsletters, number of subscribers	2 newsletters per year, 200 subscribers by the end of the project	1st newsletter (M1-M6) circulated 29 subscribers	International	
Leaflets, Brochure, Factsheet	Local/ regional/ national authorities, EC, LEAs, industrial companies, SMEs, scientific/ research community	Number of persons reached / Number of downloads (in case of virtual leaflets, considering the impact of COVID-19)	300	Materials are available Printed upon demand by partners	International	

Below, on Figure 2, Figure 3 and Figure 4 we can see the last update of PRAETORIAN's Twitter, LinkedIn and website pages.



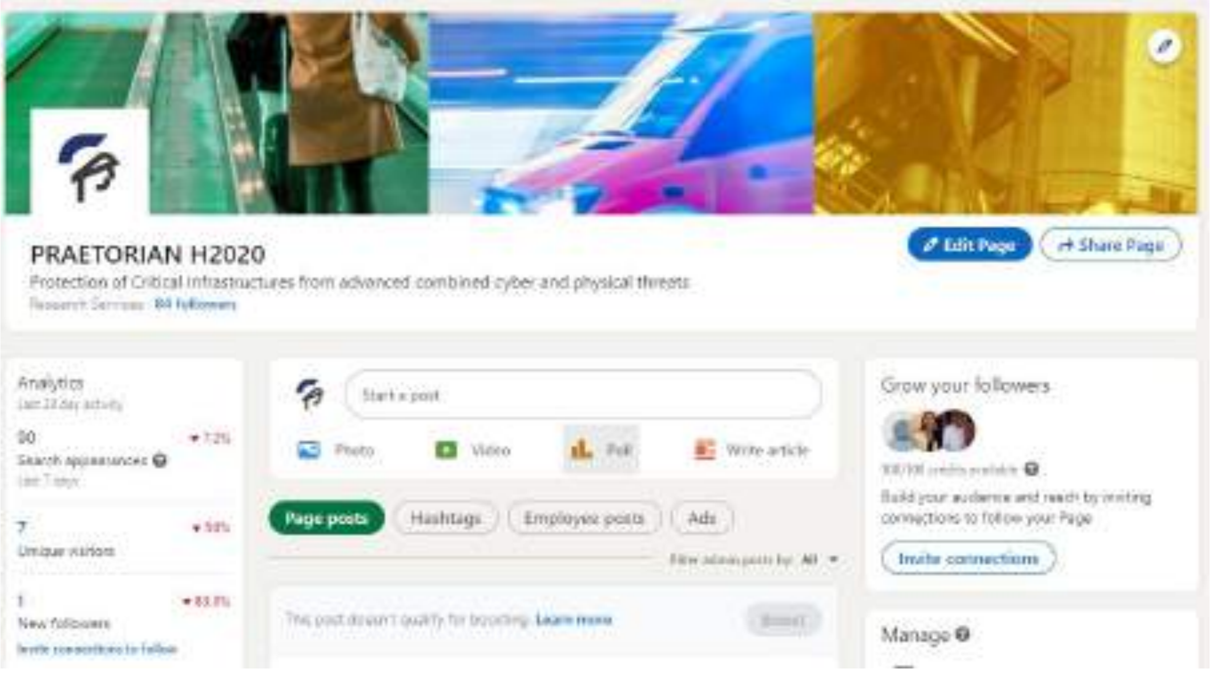
PRAETORIAN
@PraetorianH2020

PRAETORIAN project addresses and manages human-made cyber and physical attacks or natural disasters affecting CIs #H2020

Joined June 2021

26 Following 56 Followers

Figure 2. PRAETORIAN Twitter page



PRAETORIAN H2020
Protection of Critical Infrastructures from advanced combined cyber and physical threats
Research Services · 84 followers

Last 30 day activity
90 Search appearances ▾ 7.2%
Last 7 days
7 Unique visitors ▾ 50%
1 New followers ▾ 83.3%
Invite connections to follow

This post doesn't qualify for boosting. Learn more

100/100 credits available
Build your audience and reach by inviting connections to follow your Page

Figure 3. PRAETORIAN LinkedIn page

Protection of Critical Infrastructures from advanced combined cyber and physical threats

Figure 4. PRAETORIAN website page

After the end of the project, the website will be maintained by the ICCS, as a static web page. A specific brochure will be prepared at the end of the project to support the consortium members in continuing the promotion of their results and the key exploitable results of the PRAETORIAN project after its completion.

2.5.2 Community building

As was declared in the 1st version of the deliverable (D10.2), besides the planned communication and dissemination actions, PRAETORIAN partners intend to maximize the expected impact by building, maintaining, and strengthening an active PRAETORIAN Community. PRAETORIAN aims to identify and involve the representatives of CI owners and different civil society organizations and related initiatives from Europe, to maximize the creation of synergies and increase the impacts achieved by the project and the societal acceptance of the results. To this end, a targeted stakeholder engagement strategy has been employed from the beginning of the project in Task 10.5 "Community Building and Stakeholder Engagement" and as mentioned in Chapter 2.4. The members of the Community will benefit from a dedicated communication channel, in order to be informed about the early findings, to interact with consortium members, to provide valuable feedback both from the end-user and commercial perspective, to foster future synergies, and eventually to ensure a fast take-up of the developed technologies and tools. Except for the electronic communication channels that will be used for supporting the community, special workshops, demonstrations, hands-on training sessions and roundtables will be exclusively organized for its members, providing early access to tools and results and contributing to capacity building.

2.5.3 PRAETORIAN sister Projects

One equally important activity relevant to community building is the information exchange and cooperation with other similar projects under Horizon 2020 (and Horizon Europe), or else sister projects. PRAETORIAN has already identified and focused its activities to a selection of EU projects with similar objectives, as summarized in Table 3.

Of course, this table will be updated throughout the course of the project.

Table 3. Sister Projects

Project Name	Project short description	Topic	
PRECINCT	PRECINCT aims to connect private and public CI stakeholders in a geographical area to a common cyber-physical security management approach which will yield a protected territory for citizens and infrastructures.	SU-INFRA01-2018-2019-2020 - Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe	https://www.precinct.info/
SECUREGAS	SecureGas focuses on the 140.000 km 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.	SU-INFRA01-2018-2019-2020 | Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe	https://www.securegas-project.eu/
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. Critical assets are usually protected against individual physical or cyber threats, but not against complex scenarios combining both categories of threats. In order to handle it, SATIE develops an interoperable toolkit which improves cyber-physical correlations, forensics investigations and dynamic impact assessment at airports.	SU-INFRA01-2018-2019-2020 | Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe	https://satie-h2020.eu/
RESISTO	RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt),	CIP-01-2016-2017 – Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical	https://www.resistoproject.eu/

	RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters.	infrastructure of Europe	
STOP-IT	STOP-IT assembles a team of major Water Utilities, industrial technology developers, high tech SMEs and top EU R&D providers. It organizes communities of practice for water systems protection to identify current and future risk landscapes and to co-develop an all-hazards risk management framework for the physical and cyber protection of water CIs. Prevention, Detection, Response and Mitigation of relevant risks at strategic, tactical and operational levels of planning will be taken into account to generate modular solutions (technologies, tools and guidelines) and an integrated software platform.	CIP-01-2016-2017 - Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe	https://stop-it-project.eu/
INFRASTRESS	InfraStress, with its 27 partners from 11 countries, will build on preceding research towards a Technology Readiness Level 7 solution that includes threat detection, situational awareness, input from end-users and evaluation activities, presented in user-friendly services. With its integrated customised solutions, InfraStress also hopes to help cultivate a culture of participation among all involved stakeholders, from the private and public sector to civil society and citizens.	SU-INFRA01-2018-2019-2020 - Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe	https://www.infrastress.eu/
PREVISION	PREVISION has the mission to empower the analysts and investigators of LEAs with tools and solutions not commercially available today, to handle and capitalize on the massive heterogeneous data streams that must be processed during complex crime investigations and threat risk assessments.	SU-FCT03-2018-2019-2020 - Information and data stream management to fight against (cyber)crime and terrorism	http://www.prevision-h2020.eu/
DRONEWISE	DroneWISE recognizes that the illegal use of UAVs is now a serious security concern across the world as terrorists, activists and criminals are adopting drone technology and developing new, creative and sophisticated ways in which to commit crime, terrorism and invade the privacy of citizens.	ISFP-2019-AG-PROTECT (Call for proposals on protection in the	https://dronewise-project.eu/

	The adoption of drones as a tactical attack planning option for terrorists to cause mass disruption, damage economic stability and directly threaten EU security and the safety of its citizens is a chilling reminder of the clear and present danger from contemporary terrorism.	specific context of counterterrorism)	
PIXEL	PIXEL is the first smart, flexible and scalable solution for reducing environmental impacts while enabling the optimization of operations in port ecosystems through IoT. PIXEL leverages an IoT based communication infrastructure to voluntarily exchange data among ports and stakeholders to achieve an efficient use of resources in ports.	MG-7-3-2017 – The Port of the future	https://pixel-ports.eu/
ENSURESEC	ENSURESEC project aims to support the EU's vision of a reliable and trusted digital single market. It develops innovations applicable to any critical infrastructure that relies on and is monitored by networked software systems.	SU-INFRA01-2018-2019-2020 - Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe	https://www.ensuresec.eu/

2.5.4 European Cluster for Securing Critical Infrastructures (ECSCI)

In addition, PRAETORIAN has joined the ECSCI cluster, in which several projects also mentioned in Table 3 and presented in Figure 5, are members and can provide the necessary communication capabilities to the project (https://www.finsec-project.eu/ecsci). Under this light, PRAETORIAN has already participated in 2nd ECSCI workshop that took place on 27-29 of April 2022 and included presentations on novel techniques for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention, and mitigation measures.

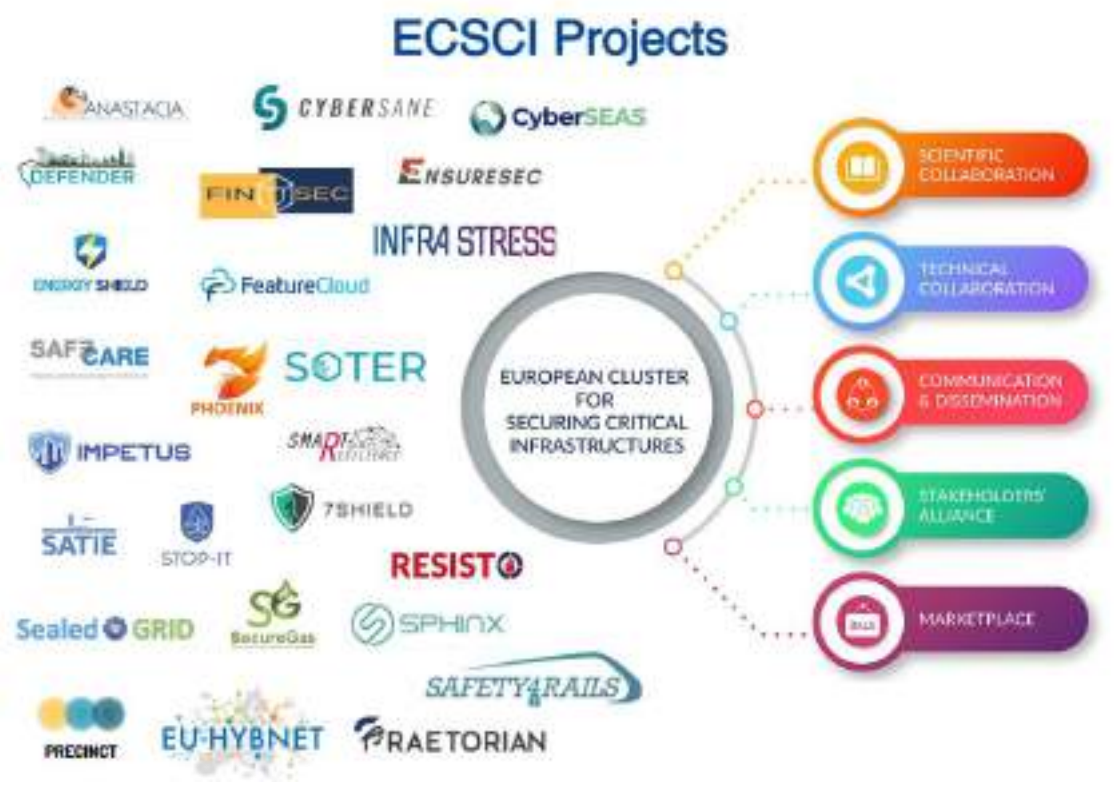


Figure 5. ECSCI Cluster members

2.5.5 Community for European Research and Innovation for Security (CERIS)

Aiming to facilitate interactions within the security research community and users of research outputs, in 2014 the European Commission established the Community of Users for Safe, Secure and Resilient Societies (CoU). This informal platform included around 1,500 registered stakeholders (policy makers, end-users, academia, industry, and civil society) and regularly held thematic events with the security research community.

In light of the forthcoming Horizon Europe developments between 2021-2027, the CoU has enlarged its scope to become the Community for European Research and Innovation for Security (CERIS).

The objectives of CERIS are to:

- Analyse identified capability needs and gaps in the corresponding areas;
- Identify solutions available to address the gaps;
- Translate capability gaps and potential solutions into research needs;
- Identify funding opportunities and synergies between different funding instruments;
- Identify standardization research-related needs;
- Integrate the views of citizens.

More information for the research Community and the future events can be found on https://ec.europa.eu/home-affairs/secure-safe-resilient-societies/index_en.

PRAETORIAN is closely watching, stays informed and participates on the events and innovations of the CERIS under the scope of dissemination and communication actions, as well as to actively contribute to this community. On 19th of October 2021, PRAETORIAN participated in a workshop organized by CERIS focusing on explosives and terrorist attacks inside the EU and more precisely, the workshop included discussions on the EU policy initiatives in this field, together with the threat and trends in Europe, Interpol activities, and trainings for practitioners. EU security research projects presented their work based on a realistic scenario developed by practitioners, from three key angles: prevention, detection and neutralization.

2.5.6 Publications

Publication and dissemination of research is an important part of the research process, passing on the benefits to a diverse range of potential beneficiaries of research, including other researchers, research sponsors, consumers and industry, policymakers, and the public. PRAETORIAN has already prepared and submitted 2 papers, also accepted, and published. During the 2nd half of the project, when more results and project outcomes will be available, we expect the number of publications to significantly rise. Publications can be found in Table 44.

Table 4. PRAETORIAN paper publications

Title	Authors	Series/Journal /Conference title	Place of publication	Date of publication
A critical review of approaches to securing proportionally to the needs and stakes – with automation considerations	Stephane Paul, Nicolas Van Cauter, Paul Varela, Simon Leboeuf and Michael Catroux	C&ESAR 2021 - Automation in Cybersecurity	Rennes	November 2021
Project PRAETORIAN	Tamara Hadjina	KONČAREVAC	Zagreb	October 2021
A Methodology for enhancing Emergency Situational Awareness through Social Media	A. Karteris, G. Tzanos, L. Papadopoulos, K. Demestichas, D. Soudris, J. P. Philibert and C. López Gómez	ARES conference 2022, (PCSCI workshop)	Vienna	August 2022

Additionally, a **PRAETORIAN newsletter** has been published to the "Critical Infrastructure Resilience: News, Updates and Events" quarterly newsletter by the EC, in June 2021.

2.5.7 Presence in Events

In general, and under the scope of the dissemination activities, partners from PRAETORIAN have participated in many events relevant to the goals and objectives of the project, such as workshops, conferences, forums, etc. For most of these events PRAETORIAN had a virtual presence, due to COVID-19 restrictions. However, there were also a few physical meetings held that gave to PRAETORIAN the chance to meet and discuss matters regarding technological innovations with experts from all around EU. The list of the events for the 1st year of PRAETORIAN's life can be seen in Table 5:

Table 5. PRAETORIAN Event participated.

Name of event	Type of event	Date	Location	Link to agenda
Protection of Critical Infrastructures from Advanced Cyber-Physical Threats: the PRAETORIAN approach	Workshop	17 August 2021	online event	https://2021.ares-conference.eu/conference-2021/detailed-program/index.html
Civil protection and safety of cities	Conference	9th and 10th September 2021	Vinkovci, Croatia	https://www.zastita.info/hr/konferencije/odrzane-konferencije/civilna-zastita-i-sigurnost-gradova/
CERIS-FCT Workshop: Explosives	Workshop	19 October 2021	online event	https://eu.eventscloud.com/website/6021/
UAV Show -Praetorian Workshop: Cyber and Physical security for critical infrastructures	PRAETORIAN booth + PRAETORIAN workshop	19, 20, 21 October	Bordeaux, France	https://www.uavshow.com/en/2021-program
Challenges for Protection of Industry and Infrastructure	Conference	27-28 October 2021	Zagreb, Croatia	https://zastita.info/hr/konferencije/izazovi-u-zastiti-industrije-i-infrastrukture-2021/program/
AI BOOST 2021	Conference	17-18 November 2021	online event	https://lithuania.lt/events/governance/ai-boost-2021/
Course name: Primer título propio de Experto universitario en Innovación y digitalización del Sector Logístico-Portuario	University course	12/17/2021	Universitat Politecnica de Valencia	-
ÉNERGIE et CYBERSÉCURITÉ : Contribuer à une meilleure résilience avec CRES	Forum	3/31/2021	Bordeaux, France	https://www.eventbrite.com/e/energie-et-cybersecurite-contribuer-a-une-

				meilleure-resilience-avec-cres-tickets-294490046657
2nd ECSCI workshop	Workshop	27 - 29 April 2022	virtual	https://www.finsec-project.eu/second-ecsci-virtual-workshop
Counter UAV Show Europe	Workshop	19 May 2022.	Sibenik, Croatia	https://cuavshow.eu/agenda/
ENSURESEC project final conference.	Workshop	20 May 2022.	online event	https://www.inov.pt/en/20-may-2022-ensuresec-closing-conference/index.html
FIC 2022 Conference	Forum	07 - 09 Jun 2022	Lille, France	https://www.forum-fic.com/en/home/
CIRCLE 2022	Conference	30 June - 1st July 2022	Gers, France	https://www.irit.fr/SIG/site/en/circle-2022-joint-conference-of-the-information-retrieval-communities-in-europe-2
PPS Event: Project to Policy Seminar	Forum	30 June - 1st July 2022	Brussels	-

2.6 When: Communication and Dissemination Plan

Active communication action has already started at the very beginning of the project and will continue during its entire life. The dates for the conferences and the professional events PRAETORIAN participated so far can be seen in Table 5. In addition, some of the events identified and are of interest of the project can be seen in Table 6; this calendar of important events will be collaboratively maintained by the consortium within the project.

Table 6. PRAETORIAN Event calendar.

Name of event	Type of event	Date	Location	Link
Participation to the Conference « ARES » for the PCSCI Workshop	Conference	23 - 26 August, 2022	Vienna, Austria	https://www.ares-conference.eu/workshops-eu-symposium/pcsci-2022/
9th Cyber and SCADA Security for Power and Utilities	Conference	20 - 21 September 2022	Virtual Event	https://www.prosperoevents.com/event/9th-cyber-scada-security-for-power-and-utilities-2022/
Lambda Mu congress λµ23	Conference	10 - 13 October 2022	Paris - EDF Labs	https://www.nae.fr/agenda/23e-ed-du-congres-%CE%BB%CE%BC-lambda-mu-du-10-10-22-au-13-10-22/

Other events which are currently organized are the following:

- **A PRAETORIAN workshop** in which the members of the Stakeholders Group and sister projects will be invited, in October 2022.
- Participation to the **PRECINCT 2nd Stakeholders workshop** in November 2022.

2.7 How: Communication Management

The communication management during the life of the project is organized with a set of ordered actions presented below: (1) Initialization, (2) Execution, (3) Monitoring & Reviewing, (4) Reporting and (5) Closing. A loop will be organized between step 2 and step 4.

2.7.1 Initialization

This step consists mainly in issuing this document, defining the communication strategy and goals, appointing the responsible management team, and designing the basic documents. This part was decided in the beginning of the project and is presented by the following:

2.7.1.1 Appoint Board / Press Office

This board had been agreed and initialized through the 1st year of the PRAETORIAN project and included in the previous deliverable D10.2 of the dissemination and exploitation plan.

Table 7. Press Office

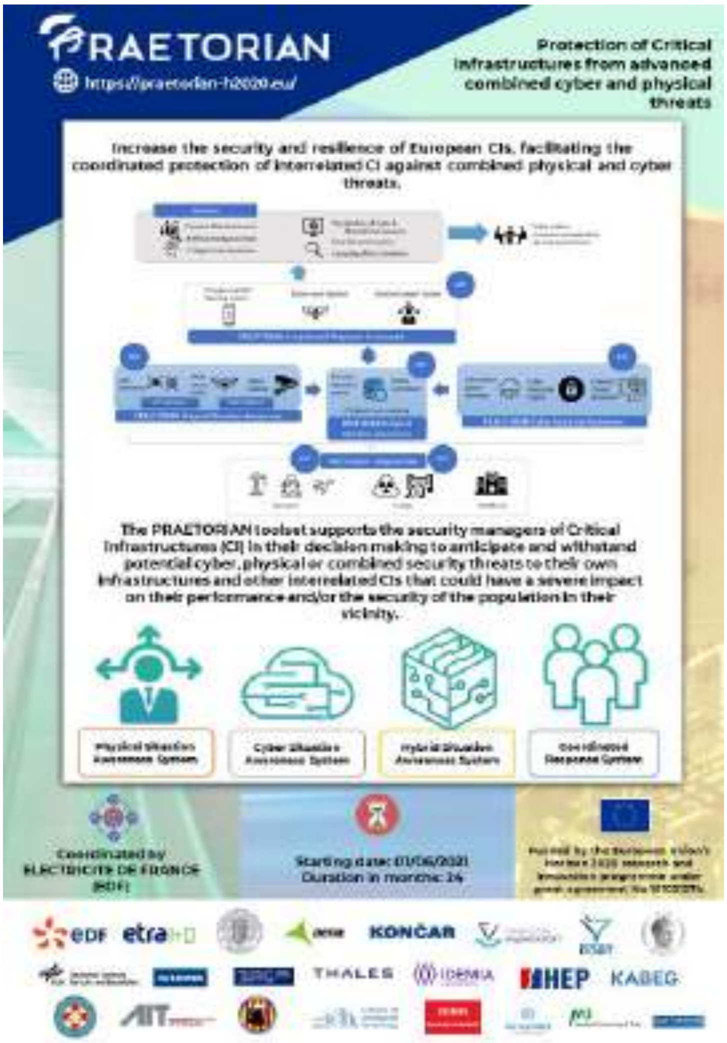
Name	Entity	Role in the Board
Konstantinos Demestichas	ICCS	Chairman and Press Office responsible
Siham Farina	EDF	Representative of Project Coordinator
Eva Muñoz	ETRA	Project Technical Manager
Wim Vandevelde	KUL	Legal and Ethics responsible
Christophe Martin	EDF	Project Security Officer (PSO)
Eva Muñoz	ETRA	WP10 Leader
Maria Carmen Bueno	ETRA	Business and Innovation Manager
Konstantina Remoundou	ICCS	Social networks administrator
Lazaros Papadopoulos	ICCS	Website admin

2.7.1.2 Defined PRAETORIAN « branding »

The branding of PRAETORIAN had been agreed and finalized through the 1st year of the PRAETORIAN project and included in the previous deliverable D10.2 of the dissemination and exploitation plan. The branding can be also found in ANNEX I.

2.7.1.3 Prepare and update of basic material

At the beginning of the project, a project leaflet (introductory brochure) and a flyer was prepared and issued to ensure efficient communication prior to the first results of the project. Furthermore, the poster is ready for communicating and disseminating PRAETORIAN activities inside conferences and public events. The poster can be seen in Figure 6.



PRAETORIAN

https://praetorian-h2020.eu/

Protection of Critical Infrastructures from advanced combined cyber and physical threats

Increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats.

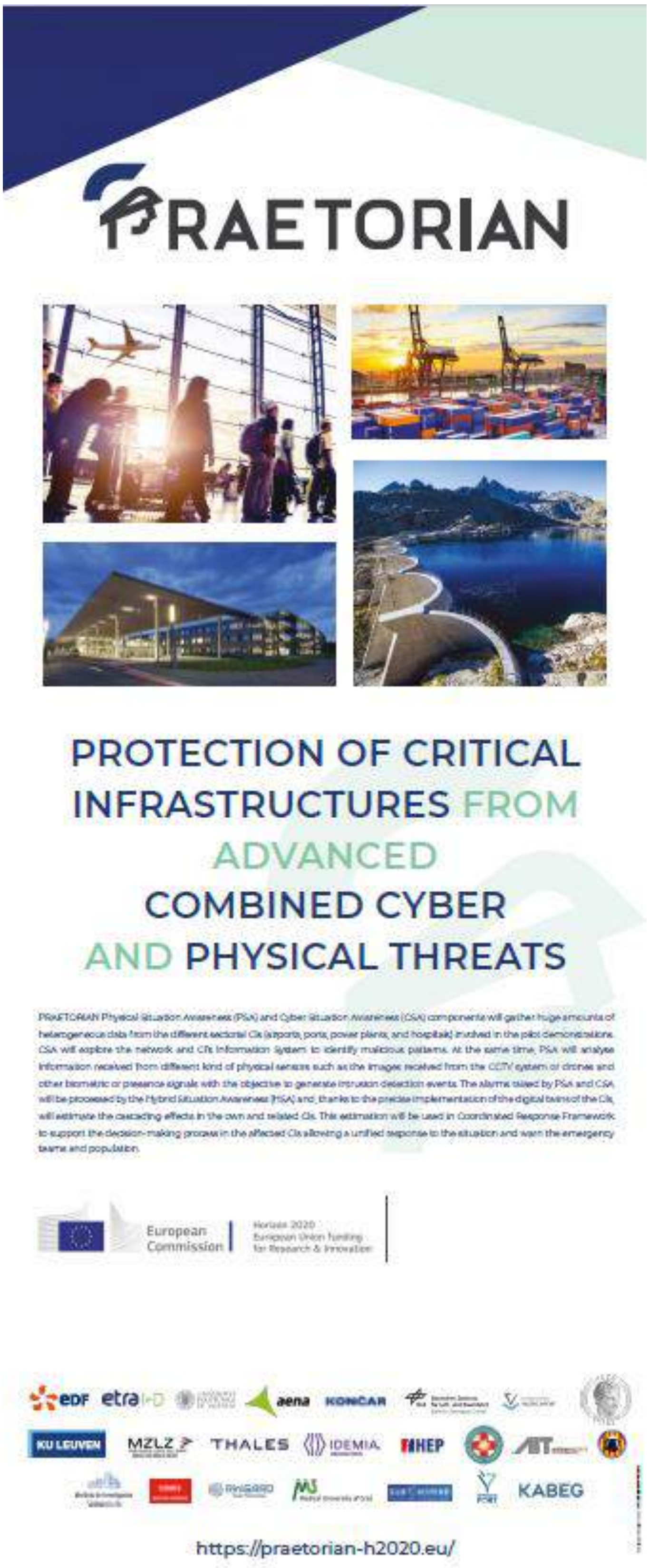
The PRAETORIAN toolset supports the security managers of Critical Infrastructures (CI) in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

Physical Situation Awareness System
Cyber Situation Awareness System
Hybrid Situation Awareness System
Coordinated Response System
EDF
etra I+D
KONČAR
THALES
IDEMIA
HEP
KABEG

Coordinated by ELECTRICITE DE FRANCE (EDF)

Starting date: 01/06/2021
Duration in months: 24

Funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021274



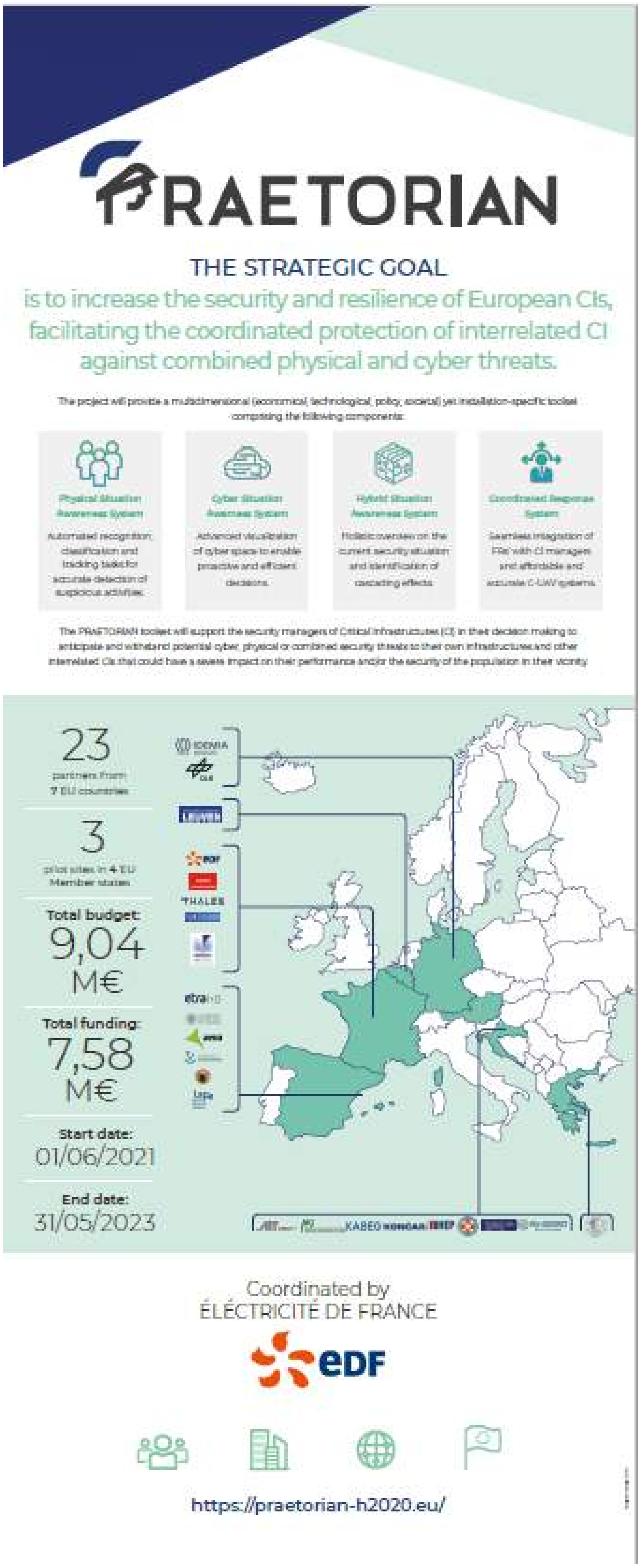
PRAETORIAN

PROTECTION OF CRITICAL INFRASTRUCTURES FROM ADVANCED COMBINED CYBER AND PHYSICAL THREATS

PRAETORIAN Physical Situation Awareness (PSA) and Cyber Situation Awareness (CSA) components will gather huge amounts of heterogeneous data from the different sectorial CIs (airports, ports, power plants, and hospitals) involved in the pilot demonstrations. CSA will explore the network and CIs Information System to identify malicious patterns. At the same time, PSA will analyse information received from different kind of physical sensors such as the images received from the CCTV system or drones and other biometric or presence signals with the objective to generate intrusion detection events. The alarms raised by PSA and CSA will be processed by the Hybrid Situation Awareness (HSA) and, thanks to the precise implementation of the digital twins of the CIs, will estimate the cascading effects in the own and related CIs. This estimation will be used in Coordinated Response Framework to support the decision-making process in the affected CIs allowing a unified response to the situation and warn the emergency teams and population.

European Commission | Horizon 2020 European Union funding for Research & Innovation

https://praetorian-h2020.eu/



PRAETORIAN

THE STRATEGIC GOAL

is to increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats.

The project will provide a multidimensional (economical, technological, policy, societal) yet installation-specific toolset comprising the following components:

Physical Situation Awareness System

Automated recognition, classification and tracking tasks for accurate detection of suspicious activities.

Cyber Situation Awarness System

Advanced visualisation of cyber space to enable proactive and efficient decisions.

Hybrid Situation Awareness System

Holistic overview on the current security situation and identification of cascading effects.

Coordinated Response System

Seamless integration of FRs' with CI managers and affordable and accurate C-UAV systems.

The PRAETORIAN toolset will support the security managers of Critical Infrastructures (CI) in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

23

partners from 7 EU countries

3

pilot sites in 4 EU Member states

Total budget:

9,04 M€

Total funding:

7,58 M€

Start date:

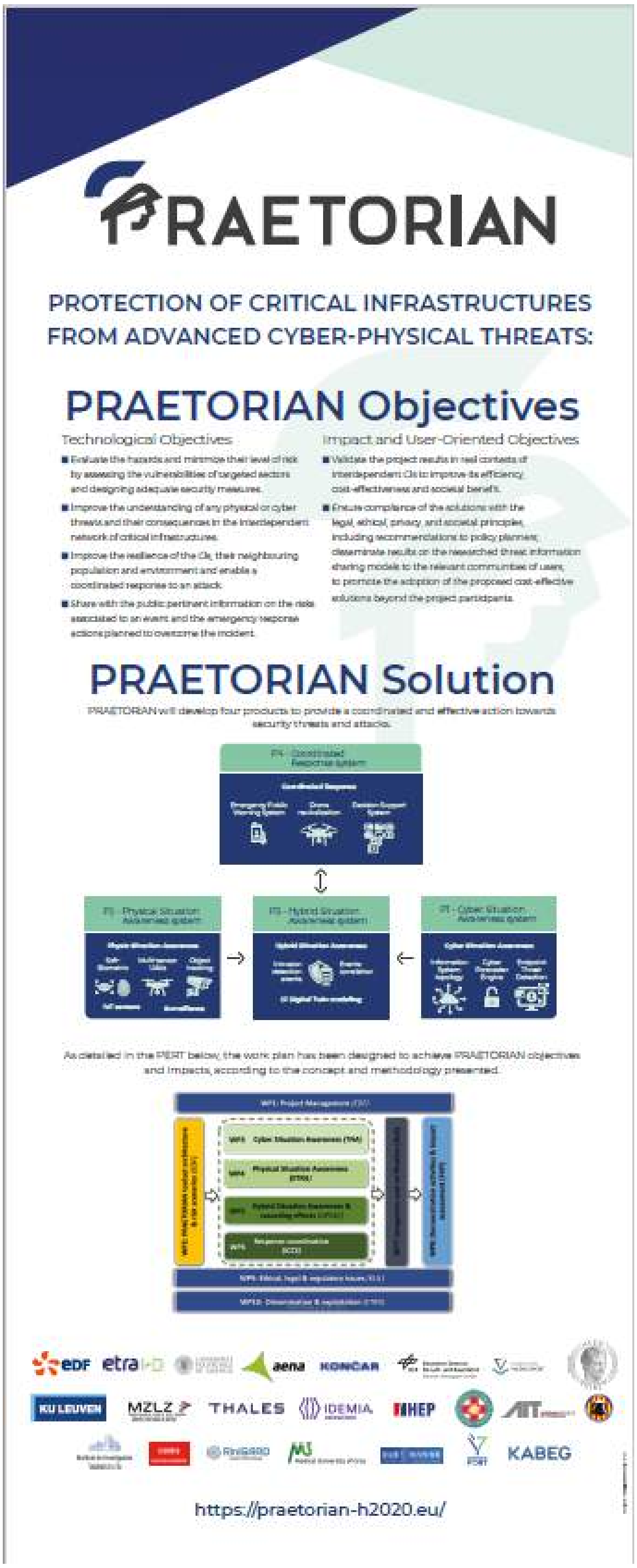
01/06/2021

End date:

31/05/2023

Coordinated by ÉLÉCTRICITÉ DE FRANCE

https://praetorian-h2020.eu/



PRAETORIAN

PROTECTION OF CRITICAL INFRASTRUCTURES FROM ADVANCED CYBER-PHYSICAL THREATS:

PRAETORIAN Objectives

Technological Objectives

- Evaluate the hazards and minimize their level of risk by assessing the vulnerabilities of targeted sectors and designing adequate security measures.
- Improve the understanding of any physical or cyber threats and their consequences in the interdependent network of critical infrastructures.
- Improve the resilience of the CIs, their neighbouring population and environment and enable a coordinated response to an attack.
- Share with the public pertinent information on the risks associated to an event and the emergency response actions planned to overcome the incident.

Impact and User-Oriented Objectives

- Validate the project results in real contexts of interdependent CIs to improve its efficiency, cost-effectiveness and societal benefit.
- Ensure compliance of the solutions with the legal, ethical, privacy, and societal principles, including recommendations to policy planners; disseminate results on the researched threat information sharing models to the relevant communities of users, to promote the adoption of the proposed cost-effective solutions beyond the project participants.

PRAETORIAN Solution

PRAETORIAN will develop four products to provide a coordinated and effective action towards security threats and attacks.

P4 - Coordinated Response system
Coordinated Response
Emergency Public Warning System
Drone neutralization
Decision Support System
P2 - Physical Situation Awareness system
Physical Situation Awareness
Safe Biometrics
Multi-purpose UAVs
Object tracking
IoT sensors
Surveillance
P3 - Hybrid Situation Awareness system
Hybrid Situation Awareness
Intrusion detection events
Events correlation
CI Digital Twin modelling
P1 - Cyber Situation Awareness system
Cyber Situation Awareness
Information System topology
Cyber Forecaster Engine
Enhanced Threat Detection

As detailed in the PERT below, the work plan has been designed to achieve PRAETORIAN objectives and impacts, according to the concept and methodology presented.

WP1: Project Management
WP3 Cyber Situation Awareness
WP4 Physical Situation Awareness (PSA)
WP5 Hybrid Situation Awareness & cascading effects
WP6 Response coordination (RCO)
WP9: Ethical, legal & regulatory issues
WP10: Dissemination & exploitation
edf
etra I+D
aena
KONCAR
KU LEUVEN
MZLZ
THALES
IDEMIA
HEP
KABEG

https://praetorian-h2020.eu/

Figure 6. PRAETORIAN posters

Also, a leaflet has been prepared explaining the overall progress of the PRAETORIAN including its Architecture description, its objectives and applications and its impact. The leaflet can be seen in Figure 7.

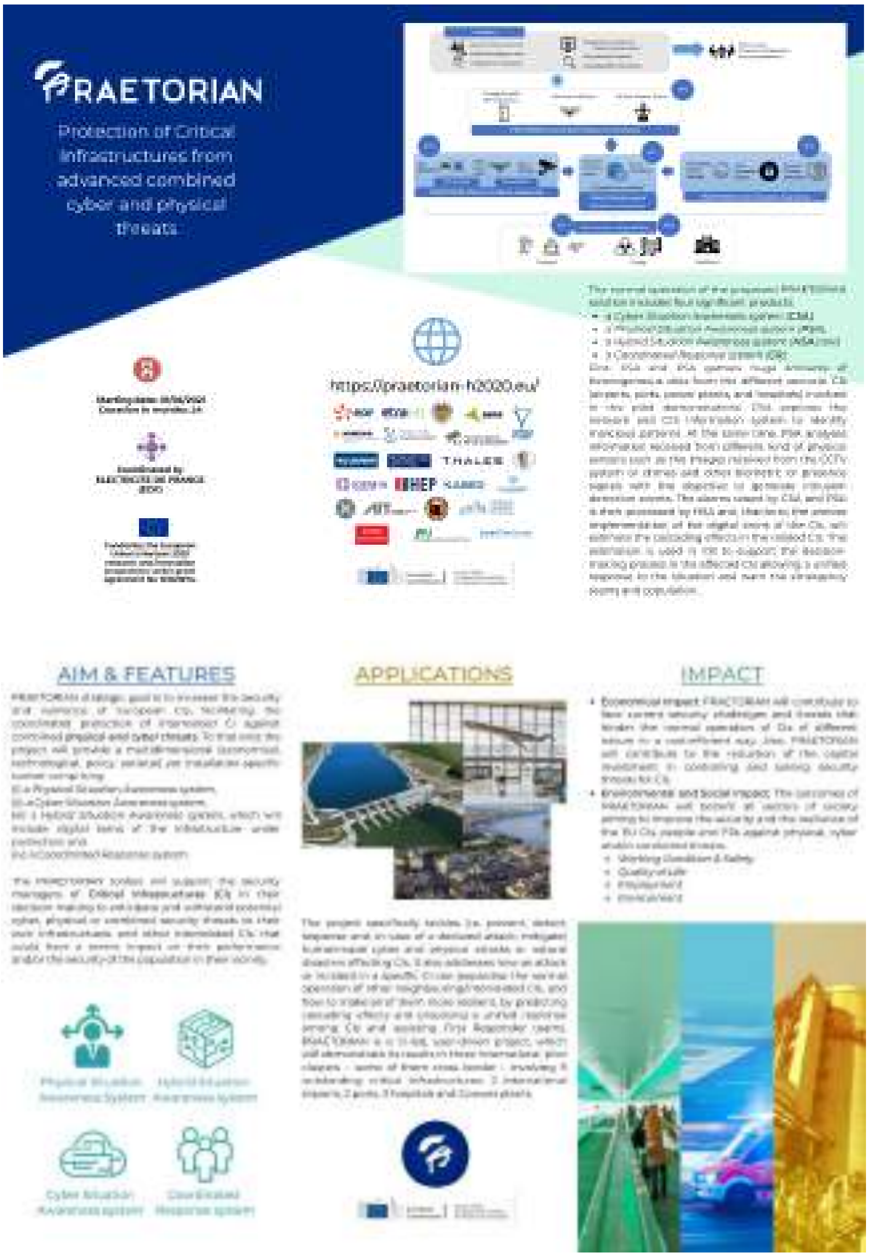
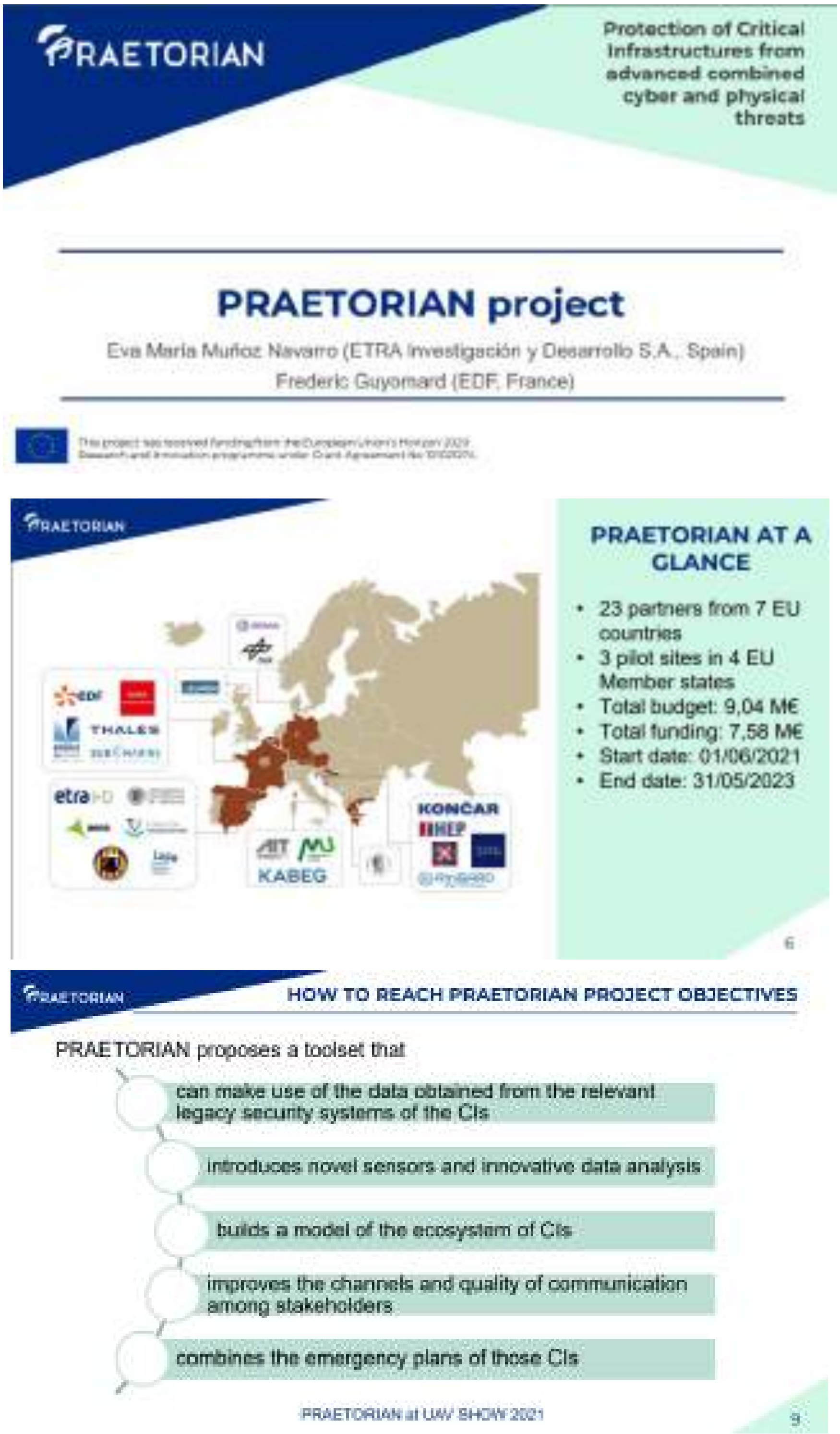

PRAETORIAN
Protection of Critical Infrastructures from advanced combined cyber and physical threats
https://praetorian-h2020.eu/
THALES
AIM & FEATURES
APPLICATIONS
IMPACT

Figure 7. PRAETORIAN leaflet

An overview of the project in presentation format is available on the website of PRAETORIAN, including information about the goals and objectives of the project, the proposed toolset that the project will provide, the partners in the consortium, the impact it will have to the stakeholders, etc. Some sampled slides can be seen in Figure 8:



PRAETORIAN

Protection of Critical Infrastructures from advanced combined cyber and physical threats

PRAETORIAN project

Eva Maria Muñoz Navarro (ETRA Investigación y Desarrollo S.A., Spain)
Frederic Guyomard (EDF, France)

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 101021274.

PRAETORIAN

PRAETORIAN AT A GLANCE

- 23 partners from 7 EU countries
- 3 pilot sites in 4 EU Member states
- Total budget: 9,04 M€
- Total funding: 7,58 M€
- Start date: 01/06/2021
- End date: 31/05/2023

6

PRAETORIAN

HOW TO REACH PRAETORIAN PROJECT OBJECTIVES

PRAETORIAN proposes a toolset that

- can make use of the data obtained from the relevant legacy security systems of the CIs
- introduces novel sensors and innovative data analysis
- builds a model of the ecosystem of CIs
- improves the channels and quality of communication among stakeholders
- combines the emergency plans of those CIs

PRAETORIAN at UAV SHOW 2021

9

Figure 8. PRAETORIAN Overview presentation sample slides

2.7.2 Execution

Following the above definition of the initialization phase, with the targeted audiences, events, locations and dates, the execution follows the below steps:

1. Prepare communication content;

2. Prepare communication support;
3. Validate through the Project Office or the WP10 participants;
4. Diffuse the communication and, if possible, obtain feedback;
5. After the communication action, archive the communication for traceability and potential reuse (please to refer to Section 2.3 for details).

For better clarity, the following cases of communication and dissemination are further distinguished:

1. **Dissemination in the form of scientific publications:** Partners should refer to article 8.5.2.1 of the Consortium Agreement (CA) about the requirements for prior notification. Partners should also make sure that they allow sufficient time between the notification (using the project's WP10 email distribution list to make their notification) and the final/official publication.
2. **Communication in the form of press releases, newsletters, etc.:** Partners should send the proposed content to the project's WP10 email distribution list allowing 1 week for reaction. If there is no objection after 1 week, partners may proceed to the publication.
3. **Communication at Social Media:**
   - **A.** In case that a partner's post is time-relevant and does not contain any actual content that could raise criticism, the partner can proceed in publishing it. Example: *I am ready to present #PRAETORIAN project at the #ARES conference. Stay tuned! #H2020 #CI*
   - **B.** In case that the partner's post contains actual content, please send it first to the Project Officer's approval email distribution list for possible objection or moderation. The partner should allow at least 24 hours for any reaction (as indicated in the members of the Project Office include the Project Coordinator, Technical Coordinator, Dissemination Manager, PSO, Ethics Manager, etc.) before posting it. Example: *#PRAETORIAN is about "XYZ" and uses "the X type of technology" to protect critical infrastructures in Europe. #H2020*. Since this candidate contains actual content/information about the approach or purpose of PRAETORIAN, it is recommended to first ask for the post to be approved.

2.7.3 Monitoring & Reviewing

This step includes monitoring and analysing the communication activities performed during specified periods in order to ensure that the PRAETORIAN partners will reach their communication goals at the end of the project. The different indicators will be computed and analysed regarding the targets of the communication activities within the specified period. The PRAETORIAN dissemination dashboard, depicted in Figure 1 is used to track and record all the communication and dissemination activities.

In case that a difficulty is identified that prevents the consortium to reach the desired target that is set in the communication and dissemination plan, then the communication plan will be updated appropriately in order to increase the effort on this failing dimension. Moreover, it should be noted that the lists of communication targets (people and events) will be reviewed and updated periodically in order to include the most recent and worth attending events/conferences (e.g., identify the dates on the conferences for the following year or add new relevant conferences).

Following the Description of Action, this document will be updated and submitted to the European Commission in M14. Results of communication, dissemination and community building actions will be published in deliverable D10.1 "Exploitation Strategy" on M28.

Table 8. Communication measures

What	Target	Reached at M14
Project website	Online by M2	https://praetorian-h2020.eu/
Twitter	Online by M2 – 150 members by the end of the project	56
LinkedIn group	Online by M2 – 100 members by the end of the project	84
PRAETORIAN community	80 members (LEAs, FRs, CI stakeholders, policy makers, other experts)	20 members
PRAETORIAN Workshop	2 workshops	A workshop will take place on October 2022
Press release including articles and publications	2 press releases per year	• The 1st newsletter has been published in social media and website. • The 2nd newsletter is under preparation
Scientific articles	5 publications in scientific journals, 10 publications in conferences/congresses	2 accepted publications in scientific projects
Project leaflet	300 physically distributed or virtually downloaded in total	Materials are available Printed upon demand by partners

2.7.4 Reporting

The last step in the loop of the communication process is reporting. In this step, a report shall be created with all the information from the previous monitoring phases. This reporting has two targets: the consortium itself and European Commission. For each reporting period, it is expected that the provided reviews regarding the PRAETORIAN dissemination and communication strategy and process will be used to revise the strategy for the next reporting period.

2.7.5 Closing

This last step will be executed at the end of the project to finalize the communication. A final deliverable D10.1 “Exploitation Strategy” will summarize the outcomes of the dissemination, communication and community building activities. Moreover, the version of the website on M28 will be kept online after the end of the project.

2.8 Crisis Communication Procedure

This section describes a set of guidelines for preventing negative publicity for the PRAETORIAN project. The PRAETORIAN consortium follows these guidelines to minimize possible effects from negative press coverage or public criticism and effectively protect the project identity.

- All press/third-party inquiries are directed to the crisis communications POC, which is expected to effectively respond the criticism, as soon as possible.

Being proactive, the PRAETORIAN consortium has taken certain measures to reduce the possibility of the development of any crisis communication:

- The PRAETORIAN consortium has designated Konstantinos Demestichas (ICCS), who guides the dissemination activities, as responsible for leading the consortium response during crisis communication (crisis communications Point of Contact - POC).
- The consortium has already identified the most sensitive technologies and activities related to privacy and data protection issues, in cooperation with the PRAETORIAN technical WP leaders, as well as with the Legal and Ethics responsible partner (KUL).
- A brief clear and accessible to a wide audience description of how the PRAETORIAN project protects data and privacy rights is under preparation and will be disseminated through the PRAETORIAN communication channels (website and social media).
- All partners agree to inform the public audience about how the PRAETORIAN project improves the security of Europe’s citizenry, while protects data sensitive for the public, as well as privacy rights.

In case of a communications crisis, ICCS will make sure that the consortium will follow the crisis communication protocol detailed here:

- Step 1: When a partner has detected a crisis communication, the ICCS POC is immediately informed. ICCS determines whether an initial conciliatory response is necessary, even before an assessment with the coordination team (EDF and ETRA) and if so, proceeds with the response.
- Step 2: ICCS and the coordination team assess together if the situation can be considered as a crisis communication.
- Step 3: If this is not the case, the process is terminated. If this is a crisis, ICCS POC has 1 week to work on the appropriate crisis plan to propose to the coordination team, which will have 2

days to accept or reject the plan. However, if the coordination team decides that a reaction must follow within a shorter period, it may take over the responsibility to respond to the crisis.

- Step 4: If the crisis plan proposed by the ICCS POC is not accepted, the coordination team makes clear amendments, which are forwarded to ICCS within 2 days. ICCS has 2 days to reply to them. The entire process cannot last longer than 10 days. When the crisis plan is accepted, it is immediately applied.

3. Summary and conclusions

This document is an update of the PRAETORIAN communication strategy and dissemination plan. Additionally, it reports all the dissemination activities during the period M1-M14. The members of the PRAETORIAN consortium actively participated in various events including conferences, workshops, and forums. The publication of newsletters, the participation in events organized by sister projects and the increased activity in social media contributed to the visibility of the projects early results. All members of the project will continue to plan and participate in dissemination activities, to reach key audiences and stakeholders and pursue collaboration opportunities with sister projects.

4. References

[1]. Guidance Social media guide for EU funded R&I projects. V1.0 – 06.04.2018

[2]. Communicating EU research and innovation guidance for project participants v1.0 – 25.09.2014

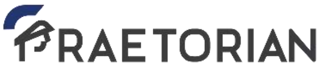
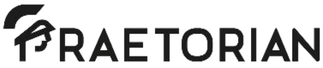
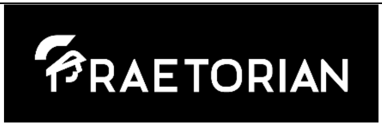
[3]. PRAETORIAN Deliverable D10.2 “Communication Strategy and Dissemination Plan v1”

Annexes

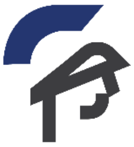
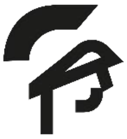
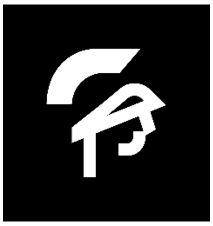
I. Initialization - Define the PRAETORIAN « branding »

The PRAETORIAN branding is defined through the set of logos below, making material distinguishable and clearly recognizable.

PRAETORIAN Logo:

 RGB	 Black	 White

PRAETORIAN Icon:

 RGB	 Black	 White

PRAETORIAN Avatar (use in social networks):