Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things

Grant Agreement: 786698

D9.2 Disseminations and use plan

Work Package 9: Dissemination and exploitation

Document Dissemination Level

P	Public	☒
CO	Confidential, only for members of the Consortium (including the Commission Services)	□

Document Due Date: 31/10/2018

Document Submission Date: 01/11/2018

Co-funded by the Horizon 2020 Framework Programme of the European Union

Document Information

Deliverable number:	**D9.2**
Deliverable title:	Dissemination and use plan
Deliverable version:	1.0
Work Package number:	WP9
Work Package title:	Dissemination and Exploitation
Due Date of delivery:	31/10/2018
Actual date of delivery:	01/11/2018
Dissemination level:	PU
Editor(s):	Stavros Shiaeles (CSCAN)
Contributor(s):	Thomas Owen, Bogdan Ghita, Stavros Shiaeles (CSCAN), Dimitrios Kavallieros, George Kokkinis, Vasiliki-Georgia Bilali (KEMEA), Emanuele Bellini, Stefano Cuomo (MATH), Nicholas Kolokotronis, Costas Vassilakis, Spiros Skiadopoulos, Christos Tryfonopoulos, Konstantinos Limniotis, Nicholas Kalouptsidis (UoP), Clement Pavue (SCORECHAIN), Elisavet Charalambous, Romeo Bratska (ADITESS), Raymond Binnendijk (CGI), Xenia Pouli (MTN).
Reviewer(s):	Gohar Sargsyan (CGI), Emanuele Bellini (MATHEMA)
Project name:	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Project Acronym	Cyber-Trust
Project starting date:	01/05/2018
Project duration:	36 months
Rights:	Cyber-Trust Consortium

Version History

Version	Date	Beneficiary	Description
0.1	27/08/2018	CSCAN	Proposed outline
0.2	01/10/2018	All	Partners Input
0.3	22/10/2018	CSCAN	Submitted for review
0.4	29/10/2019	CGI, MATHEMA	Review
0.5	31/10/2018	CSCAN	Final review and address reviewer comments
1.0	1/11/2018	KEMEA	Final review and Submission

Acronyms

ACRONYM	EXPLANATION
API	Application Programming Interface
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
COA	Course of Action
CPE	Common Platform Enumeration
CSIRT	Computer Security Incident Response Teams
CTI	Cyber-Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVRF	Common Vulnerability Reporting Framework
ENISA	European Union agency on network and information security
KPI	Key Performance Indicators
RTD	Research and Technological Development

EXECUTIVE SUMMARY

The Internet has grown exponentially in terms of size, complexity, and functionality since its inception and, over the past decade, the interfacing with the Internet environment has also changed dramatically. The interface devices moved from traditional computers with large hardware footprint and significant computational abilities towards mobile devices, of comparable computation strength and, more recently, towards Internet of Things devices that allow existing equipment, from cars through to fridges and wind turbine sensors, to have an Internet presence. The potential that this Internet of Things has on the development of new technologies is yet difficult to fully forecast; however, together with its benefits, come the familiar dangers posed by cyberthreats, whether from state sponsored attacks or criminal organisations seeking to maximise financial reward. Unlike more established, fixed or mobile, computing hardware, IoT also bears rather limited abilities to protect and upgrade, which leads to further problems when trying to ensure an attack-free environment.

Cyber-Trust was established as part of a European Union funded endeavour to identify and mitigate the effects of cyber threats against the Internet of Things. Rather than trying to change the devices, it accepts the premise that the IoT environment encompasses inherent weakness, therefore it establishes an infrastructure to ensure the protection and security of the environment is in place, in spite of the existing vulnerabilities. It aims to:

1. Create a new paradigm for the next generation Cyber Security systems, especially suited for the IoT, that will greatly increase the capability of CIIs to counter threat actors and their methods.
2. Swiftly detect and effectively respond to/mitigate sophisticated cyber-attacks by advancing the current state-of-the-art of numerous existing techniques and by introducing new ones.
3. Deliver advanced solutions for collecting forensic information from the defending systems to identify the attackers and further use it as evidence in court.
4. Minimize the impact on sensitive data protection and user’s privacy of the proposed tools and methods by addressing any issues during the design and the development phases.

A stated deliverable of this project is the development of a dissemination strategy that outlines how Cyber-Trust intends to communicate the research and development that is conducting to a wide range of stakeholders, ranging from government departments and Cyber Security researchers through to SMEs and wider society. The following document outlines this strategy in further detail, as well as providing guidance to the various project partners and Cyber-Trust consortium members.

Contents

List of figures

List of tables

1. Introduction

The following pages constitute the dissemination and communication strategy designed to articulate how the Cyber-Trust Consortium plans to disseminate the research it is conducting and the conclusions it is drawing. Its primary audience will be the Consortium Partners, but it will also serve as a guide for interested parties wanting to know how to access this information when it is available.

It will be strategic in nature, meaning it will provide granular detail about when podcasts or blogs will be released. It will instead provide an overview of what information the Consortium aims to communicate, how it intends to communicate it, and the type of input expected of Consortium Partners. However, Key Performance Indicators (KPIs) for each dissemination tool will be provided to set an initial goal for partners, ensuring that Cyber-Trust activities and research outcome are disseminated effectively.

When developing content to be disseminated partners should bear the following points in mind:

- **Plan**: decides on the target group to reach and how, the tools to utilise and the key messages to establish;
- **Design**: implements the communication methods, allocates the required resources, and assigns responsibilities;
- **Evaluate**: monitors the quality measures / indicators and compares the goals against the achieved results;
- **Adjust**: adjusts the plans for future communications accordingly based on the outcome of the evaluation.

To that end the document is divided broadly into three distinct sections.

- The first section covers what type of information will be communicated and who it will be communicated to, with a caveat describing restrictions relating to commercial sensitivities.
- The second section covers the tools the Consortium will use to disseminate that information
- The third section will cover the responsibility each Consortium partner has to disseminate information that is relevant to the project outputs.
- Finally, the document will conclude by looking at Key Performance Indicators and the advisory board as well as their role in the dissemination of Cyber-Trust.

1.1 Document Purpose

This document will form the core dissemination and communication strategy for all Cyber-Trust's activities throughout the life of the project. It will contain detailed information on partners, stakeholders, methods of communication and any restrictions to dissemination due to commercially sensitive information. The document will be then used as a reference to evaluate the progress of the project during its lifecycle.

2. Dissemination and use plan

This section describes the dissemination use plan in terms of objectives, key target audience as well as the key message the Cyber-Trust project envisioned to circulate.

2.1 Dissemination objectives

This dissemination plan consists of several stated objectives to be met over the life of the project, the key stakeholders that will be targeted, the scope of the activities and the roles of the project partners. This section describes all these components, as well as an outline of the strategy based on the Description of Action.

Stated objectives:

1. Raise awareness on the Cyber-Trust project and its achievements by employing a diverse range of communication strategies.
2. Impact on the technology roadmap and future research on Cyber Security by participating in expert forums, publishing in conferences/journals, and contributing to standardization.
3. Improve the awareness of the European industry and SMEs on Cyber Security domain and help them make better use of the project results through targeted dissemination tools.
4. Cyber Security industry – project platform and tools to raise security and prevention of malware attacks, minimizing the impact of the attack and the data loss.

2.2 Key message

***"You can have brilliant ideas, but if you can't get them across, your ideas won't get you anywhere."* – Lee Iocacca**

The key message of the project is crucial to unifying the communication from partners to the wider target audience and should underpin every form of communication made by the Consortium. Broadly, the project's key message is this:

"Cyber-Trust's raison d'etre is to create a new paradigm shifting platform for the next generation of Cyber Security systems, engineered specifically for the Internet of Things, that will greatly increase the capability of organisations of all types to counter threat actors and their methods. It will look to quickly detect and effectively respond to and mitigate sophisticated cyber-attacks by developing cutting edge techniques and building on previous best-practice. Cyber-Trust aims to deliver advanced solutions for collecting forensic information from the defending systems to identify the attackers and further use it as evidence in court. Crucially it will minimize the impact on sensitive data protection and user's privacy of the proposed tools and methods by addressing any issues during the design and the development phases."

2.3 Target audience

In any communications plan, the target audience is key to the success of the project and its longevity beyond the proposed end date. Therefore, considerable effort has been made to identify which groups are going to benefit the most from this project. They are:

1. **European Commercial and Industrial stakeholders**: These are commercial and industrial based predominantly within the European Union whose day-to-day activities could be positively impacted by the results of the Project.
2. **Internet Service Providers (ISPs):** These companies are at the heart of the internet infrastructure, the providers of internet services to the vast majority of users around the world. As they are key in the development of the Internet of Things, consideration must be made for their interests.
3. **Law Enforcement Agencies (LEAs) and Governmental agencies:** LEAs and Cyber Security Response Teams (CSRT) in Europe will gain valuable knowledge in regards with identification and mitigation of cyber-threats/attacks, sharing of information as well as possible deployment of Distributed Ledger Technologies (DLT) in the field of digital forensics.
4. **Cyber Security Research Community**: This include researchers in academia, PhD students as well as those individuals devoted to researching Cyber Security area, whether in support of academic projects, private companies or as a contribution to open-source Cyber Security projects.
5. **Other running projects**: Research and development projects in similar research focus and interest. Results will be discussed identifying common problems, exchange information, receive and provide feedback.
6. **EU citizens:** This refers to the wider public and non-scientific audience that wishes to be informed regarding the material and tools Cyber-Trust will produce.
7. **IT professionals:** a group of specialists who build, maintain, and repair the Cyber Trust's system. They should also have a significant level of skill and knowledge in the Cyber Security field.

The following table highlights a broad cross section of the type of audience Cyber-Trust expects to engage with and the added value Cyber-Trust will add to them and vice versa.

Table 3.2.1: Cyber-Trust target group and added value

Target group	Cyber-Trust added value
European Commercial and Industrial stakeholders	Marketing campaigns to increase public awareness and promote project's approach.
Internet Service Providers (ISPs)	The companies see how to use the Cyber-Trust and provide a secured service of Internet thereby increasing the trust of users in these companies.
Law Enforcement Agencies (LEAs) and Governmental agencies	These Agencies will get a better view about how to achieve fundamental actions in identifying and then mitigating the threats thereby saving their time and efforts.

Cyber Security Research Community	The researchers can contribute with new ideas to propose solutions for current issues in the Cyber Security domain. These ideas can cover the vulnerabilities of Internet Service Providers.
Other running projects	The industrial partners will use their well-established networks of international (and national) contacts to communicate the results of Cyber-Trust project, draw their attention and increase its visibility.
EU citizens	The EU citizens can easily get services and new updates through their IOT devices. The project will help them to identify the issues with their network and devices with simple messages thereby understanding the problem and how can be solved.
IT professionals	The IT professionals can solve any issues that might happen with system and recover all services immediately.

3. Dissemination and Communication Tools

Dissemination tools describe how the research findings of the Consortium are communicated to the target audience. While no distinction is made between different audience groups, it is important to recognise that certain audience groups will be reached by utilizing certain tools. It will also look at how the Consortium's dissemination activities impact on other Horizon2020 projects that are running concurrently.

3.1 Project Website

The Cyber-Trust public website is one of the key communication tools (please see D9.1 Cyber-Trust project website). It serves as a public window, in which the project communicates relevant information about its goals, progress, etc. The website also includes features like search and article categorization for improved content discovery. As another means for increasing communication between the consortium and third parties, a blog page is also maintained as a section within the webpage. Blog posts should involve aspects or conventions related to the project, including more extensive descriptions about project achievements and demo versions. Additionally, the blog page may serve as a means of increasing the traffic of the page and a reason for visitors to check back the website at a later stage.

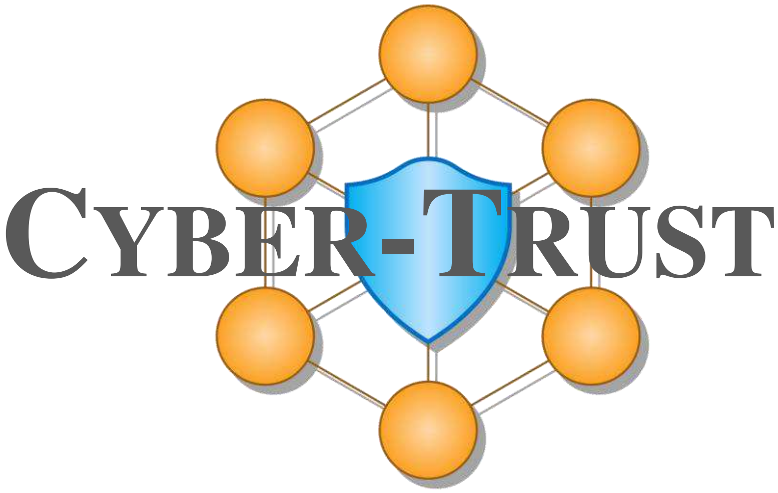
The primary objective of the website is to provide a convenient and easy-to-access repository of information regarding the project's aims and its findings and is a key component of the dissemination process.

The website will be continually updated with information regarding research papers, blog posts, podcasts, and news of events that members of the project team will be attending. In addition, and with permission from the blog creator, the website will re-publish blogs written by individuals involved in the project or provide links to the original content.

ADITESS, has the responsibility for the technical maintenance of Cyber-Trust website (www.Cyber-Trust.eu) and social media accounts (Twitter, YouTube, LinkedIn and Facebook). ADITESS will therefore be responsible for the uploading of content provided by the Cyber-Trust consortium through the dissemination manager CSCAN.

3.2 Cyber-Trust logo/flyer design

The Cyber-Trust logo represents the visual identity of the project enhancing the recognition of the project and its visibility. The following figure depicts different version of the logo.



RGB: 253, 180, 80 HEX: FDB450	RGB: 32, 184, 242 HEX: 20B8F2	RGB: 89, 89, 89 HEX: 595959

Figure 3.1: Cyber-Trust Logo and graphical items

The main aim of the Cyber-Trust flyer and poster is to disseminate the main aim and goal of the project, to highlight the innovations, the research areas as well as the overall benefits of the project. The first flyer is composed by one page depicting the aforementioned information. Both, the flyer and the poster can be found in Annex A Cyber-Trust Flyer and B Cyber-Trust Poster, respectively.

3.3 Email Digests

Cyber-Trust website will be integrated with the MailChimp service to allow subscription of visitors to a dedicated Cyber-Trust mailing list. MailChimp allows the users to opt in and out of communication at any time and therefore provides the required flexibility for compliance with the GDPR.

The project website will be configured to release email digests every three months starting from M9 with project updates, blog posts and events to which consortium members participated. ADITESS will be responsible for the configuration of this tool while CSCAN as the dissemination manager will be responsible for the provision of content to be published.

The email digests will serve as an additional dissemination channel to reach interested parties.

3.4 Social Media

ADITESS, in conjunction with CSCAN, will be responsible for the running of Cyber-Trust social media accounts, to include Twitter, LinkedIn, Facebook and YouTube. Twitter is the platform of choice for the communication of all website updates and key project updates. An account has been created @cybertrusteu (created in May 2018). Partner organisations and individuals are encouraged to like and retweet any updates to maximise the exposure of Cyber-Trust and its activities. LinkedIn is the platform of choice for updates pertaining specifically to government and industry (an account is yet to be created), and YouTube will be used for the publishing of any video content, including, but not limited to, video-conferences, as well as footage from any relevant seminars and lectures.

The CSCAN team will also endeavour to hold regular YouTube Live sessions, that will allow interested parties to submit questions and provide feedback to the team regarding released research.

Table 3.1: Cyber-Trust Social Media Accounts

SM Account	Name	Link
Facebook Page	CyberTrust	https://www.facebook.com/cybertrust/
Twitter	CyberTrustEU (@CyberTrustEU) (#CyberTrust)	https://twitter.com/CyberTrustEU
Linkedin	CyberTrustEU	https://www.linkedin.com/groups/13627755/
YouTube	CyberTrustEU	https://www.youtube.com/channel/UCgxDwNbPM0SXJciOkkdoAiA?view_as=subscriber

3.5 Blogs

Blog posts will be used in place of a traditional 'press release' for all project related updates and research findings. It will be the primary tool for updating interested parties to our progress. Should a press briefing involving journalists be required, this will be dealt with in a special discussion with partners if and when the need arises.

The personal blogs of individual project members, as well as blogs run by the academic and industrial partners are vital to disseminating the activities of the consortium. The publishing of guest blogs on prominent tech websites is also encouraged, particularly those focused on Cyber Security and technological innovation.

It is the aim of the communications team to release at least 10 blog throughout the project life as a broad update on the project, with specific "special edition" blogs being release when necessary.

3.6 Newsletters

Periodic newsletters will be produced bi-annually starting at M7 of the project, providing news, articles, and in-depth information about the project progress and outcomes, and any other relevant information that applies at the time of the publication. The newsletters will present the several activities undertaken by Cyber-Trust, describing the project developments, the deliverables' findings and the results that will be reached step-by-step, and they will provide suggestions coming from the project's meetings and the partners' collaboration. The process of the newsletter production will be based on the following steps:

- CSCAN will design the newsletter template
- All partners will provide suggested content for the newsletter to CSCAN
- CSCAN will review/edit and prepare the draft version of the content for the newsletter issue
- ADITESS will review/edit and develop the final draft version that will be sent to KEMEA as Project Coordinator
- KEMEA will review/edit and approve the content of the issue and provide authorisation for publication
- ADITESS will fit the content to the newsletter template and publish the newsletter in the Cyber-Trust website
- All partners will disseminate the newsletter in National and International interest groups

The newsletter will be A4 sized, and it is supposed to be constituted by 2 to 4 pages, in order to be printable in a single leaf, and to be easily folded. However, the length of the newsletter may exceed the 4-pages limit, depending on the number of news and articles to be published.

3.7 Press Releases

Local press is another communication channel that will be used in the project. All partners will put additional effort to release the project concept, scope, objectives and expected outcomes in local press in UK, Greece, Luxemburg, Cyprus, Italy and Netherlands. CSCAN is the responsible partner to develop press releases in the English language. In accordance with the Communication roadmap, press releases will be prepared in M12, M24 and M36. All partners will interpret the press releases in their local language. Any expenses will be covered by the project budget.

3.8 Podcasts /Promo Video/Webcasts

Cyber-Trust team will also hold Podcast sessions that will discuss the Project and its findings and place it in the wider context of Cyber Security, with a view to reinforcing the importance of the project to the wider field of security, and not just limited to the Internet of Things.

3.9 Project Stationery

There will be a need to develop a plethora of tertiary communications tools such as the design and creation of conference paraphernalia such as brochures, flyers, infographics, posters and banners.

3.10 Cyber-Trust GitHub

Cyber-Trust is committed at delivering open-source software and therefore the source code of the components of the Backend Framework will be pushed to a Github repository that will be created when the first round of developed components will be released. ADITESS will be responsible for the creation and maintenance of this repository and all source control tools. Github will also serve as a dissemination and exploitation channel for the community of software and security developers. Through Github Cyber-Trust may share publicly accessible technical information and code for the benefit of the wider Cyber Security community.

4. Planned Dissemination and Communication Activities

4.1 Publications

As a research project the publication of the project's development and results in high-quality journals is one of the main priorities of the partners since the beginning of the project. The following tables presents an indicative list of journals that are relevant to the Cyber-Trust research areas. It is important to highlight that the following list is non-exhaustive, and the submission of articles will be based on whether a journal's specific topics (or call for papers in special issues) match those of the particular work carried out in the context of Cyber-Trust.

Table 4.1: Scientific Journals

Title of Journal	Aim	Web-site
Transactions on Dependable and Secure Computing (IEEE Xplore)	The purpose of TDSC is to publish papers in dependability and security, including the joint consideration of these issues and their interplay with system performance	ieeexplore.ieee.org
Transactions on Information Forensics and Security (IEEE Xplore)	The IEEE Transactions on Information Forensics and Security covers the sciences, technologies, and applications relating to information forensics, information security, biometrics, surveillance and systems applications that incorporate these features	ieeexplore.ieee.org
IEEE Security & Privacy	IEEE Security & Privacy's primary objective is to stimulate and track advances in security, privacy, and dependability and present these advances in a form that can be useful to a broad cross-section of the professional community—ranging from	ieeexplore.ieee.org

	academic researchers to industry practitioners	
IET Information Security	IET Information Security publishes original research papers in the following areas of information security and cryptography	ieeexplore.ieee.org
International Journal of Information Security	The Journal offers prompt publication of high quality research on *system security* (intrusion detection, operating system security, database security), *network security* (Internet security, firewalls, mobile security, security protocols, anti-virus), *foundations* (privacy, access control, authentication, identification, applied cryptography, and formal security methods).	https://link.springer.com/journal/10207
Computer Fraud & Security (Elsevier)	Computer Fraud & Security enables you to see the threats to your IT systems before they become a problem. It focuses on providing practical, usable information to effectively manage and control computer and information security within commercial organizations	www.journals.elsevier.com/computer-fraud-and-security
Computer Law & Security Review (Elsevier)	The Computer Law and Security Review (CLSR) is an international journal of technology law and practice providing a major platform for publication of high-quality research, policy and legal analysis within the field of IT law and computer security	www.journals.elsevier.com/computer-law-and-security-review
Computers & Security (Elsevier)	Computers & Security is the most respected technical journal in the IT security field. With its high-profile editorial board and informative regular features and columns, the journal is essential reading for IT security professionals around the world	www.journals.elsevier.com/computers-and-security
Network Security (Elsevier)	Network Security is devoted to solving your network security issues in detail, now with even more news, information and solutions to your network security problems	www.journals.elsevier.com/network-security
International Journal of Information	The journal focuses on publishing articles that address the paradoxical nature of privacy versus security amidst current	www.tandfonline.com/toc/uips20/current

Security and Privacy (Taylor & Francis)	global conditions. It is increasingly important that various constituents of information begin to understand their role in finding the delicate balance of security and privacy	
Journal of Physical Security	The Journal of Physical Security (JPS) is a free, non-profit, online, peer-reviewed journal devoted to physical security R&D, testing, evaluation, analysis, theory, modeling, and management. Both technical and social science aspects of physical security are of interest	rbsekurity.com/the-journal-of-physical-security.html
Journal of the ACM	The Journal of the ACM (JACM) provides coverage of the most significant work on principles of computer science, broadly construed	https://jacm.acm.org/
International Journal of Human-Computer Studies	Publishes original research over the whole spectrum of work relevant to the theory and practice of innovative interactive systems	https://www.journals.elsevier.com/international-journal-of-human-computer-studies
Computers and Society	The most respected technical journal in the IT security field. With its high-profile editorial board and informative regular features and columns, the journal is essential reading for IT security professionals around the world	https://www.journals.elsevier.com/computers-and-security
Computer Law & Security Review	Is an international journal of technology law and practice providing a major platform for publication of high quality research, policy and legal analysis within the field of IT law and computer security	https://www.sciencedirect.com/journal/computer-law-and-security-review
ACM Transactions on Information and System Security	Devoted to the study, analysis, and application of information and system security. TISSEC topics include: security technologies; secure systems; secure applications; and security policies	https://dl.acm.org/citation.cfm?id=J789
Designs, Codes and Cryptography (DCC)	Designs, Codes and Cryptography provides a forum for high quality papers of both a theoretical and a practical nature which bridge more than one of these areas, encouraging interaction between them.	https://link.springer.com/journal/10623

Cryptography and Communications (CCDS)	Cryptography and Communications Discrete Structures, Boolean Functions and Sequences (CCDS) publishes high-quality papers discussing cryptography, error correcting codes, communications and their interactions.	https://link.springer.com/journal/12095
Journal of Cryptology	The Journal of Cryptology is a forum for original results in all areas of modern information security. Both cryptography and cryptanalysis are covered, including information theoretic and complexity theoretic perspectives as well as implementation, application, and standards issues.	https://link.springer.com/journal/145
Journal of Mathematical Cryptology	The *Journal of Mathematical Cryptology (JMC)* is a forum for original research articles in the area of mathematical cryptology. Works in the theory of cryptology and articles linking mathematics with cryptology.	https://www.degruyter.com/view/j/jmc
ACM Transactions on Information Systems (TOIS)	Information Systems (TOIS) is a scholarly journal that publishes previously unpublished high-quality scholarly articles in all areas of information retrieval.	https://tois.acm.org/
IEEE Transactions on Knowledge and Data Engineering (TKDE)	The scope includes the knowledge and data engineering aspects of computer science, artificial intelligence, electrical engineering, computer engineering, and other appropriate fields.	https://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=69
Large-Scale Data- and Knowledge-Centered Systems (TLDKS) - Springer	The objective of the international journal on Large Scale Data and Knowledge Centered Systems is to provide an opportunity to disseminate original research contributions and a high quality communication platform for researchers and practitioners.	https://www.irit.fr/tldks/
The VLDB Journal - Springer	The VLDB Endowment journal contains scholarly contributions that examine information system architectures, the impact of technological advancements on information systems, and the development of novel database applications.	https://link.springer.com/journal/778

Information Processing and Management (IPM) - Elsevier	Information Processing and Management is a leading international journal focusing on publishing peer-reviewed original research concerning theory, methods, or application in the field of information science.	https://www.journals.elsevier.com/information-processing-and-management

4.2 Participation at Conferences, Events and Industrial Expos

All consortium partners will be required to attend events that are relevant to the project and offer an opportunity to communicate the aims and current findings of the project.

Academic Partners will be required to actively seek out these events in their host nation, and coordinate with the communications team regarding overseas events.

All industrial partners will be required to attend any business expos and conferences relevant to their industry area and their contribution to the project.

While all partners will be free to choose which events, they attend and the nature of their attendance, it is required that any information given out by attendees (flyers, brochures etc.) be approved by the communications team.

Table 4.2: Conference list

Title of Conference	Web-site	Frequency	Next
FS-ISAC ANNUAL SUMMIT	www.fsisac-summit.com/2019-Annual-Summit-Overview	Annual	2019
CANSECWEST	cansecwest.com	Annual (usually every March)	2019
Hack in the Box Security Conference	conference.hitb.org	Annual	2019
APPSEC EUROPE	2018.appsec.eu	Annual	2019
FIRST Annual Conference	www.first.org/conference		2019
CanSecWest			
BLACK HAT Europe	www.blackhat.com	Annual	2018
Annual Industrial Control Cyber Security Europe	cybersenate.com	Annual	2019
Cyber Security Week – The Hague	https://www.cybersecurityweek.nl	Annual	2019
Cyber London Conference I	www.cyberlondonconference2018.com	Annual	2018
DevSecCon London	www.devseccon.com/london-2018	Annual	2018

FT Cyber Security Summit	live.ft.com/SERIES/FT-Cyber Security-Summit	Annual	2019
R3: Resilience, Response & Recovery Summit	r3summit.co.uk	Annual	2019
Security and Trust Management	www.nics.uma.es/pub/stm18/	Annual	2019
Europol-ENISA IoT Security Conference	https://www.enisa.europa.eu/events/enisa-europol-internet-of-things-conference	Annual	2019
IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2018)	http://cyber-science.org/2018/dasc/	Annual	2019
ACM Dependable, Adaptive, and Trustworthy Distributed Systems	http://www.dedisys.org/sac19/	Annual	2019
Int'l Conference on Decision and Game Theory for Security (GameSec)	http://www.gamesec-conf.org	Annual	2019
USENIX Security Symposium	https://www.usenix.org/conference/usenixsecurity19	Annual	2019
IEEE Symposium on Security and Privacy	https://www.ieee-security.org/TC/SP2019/	Annual	2019
IEEE European Symposium on Security and Privacy	https://www.ieee-security.org/TC/EuroSP2019/	Annual	2019
Annual Privacy Forum (organized by ENISA)	https://privacyforum.eu/	Annual	2019
Privacy Enhancing Technologies Symposium (PETS)	https://petsymposium.org/	Annual	2019
International Conference on Information Systems Security and Privacy (ICISSP)	http://www.icissp.org/	Annual	2019
International Conference on Cryptography and Security in Balkans (BalkanCryptSec)	https://www.bcs2018.org/	Biannual	2020
IEEE International Conference on Blockchain and Cryptocurrency (ICBC)	http://icbc2019.ieee-icbc.org/	Annual	2019
Financial Cryptography and Data Security (FC)	https://fc19.ifca.ai/	Annual	2020
ACM Conference on Computer and	https://www.sigsac.org/ccs/CCS2018/	Annual	2019

Communications Security (ACM CCS)			
ACM Asia Conference on Computer and Communications Security (ACM AsiaCCS)	http://asiaccs2018.org/	Annual	2019
ACM International Conference on Management of Data (SIGMOD)	http://sigmod2019.org/sigmodcfp	Annual	2019
ACM International Conference on Web Search and Data Mining (WSDM)	http://www.wsdm-conference.org/2019/	Annual	2019
ACM Conference on Research and Development in Information Retrieval (SIGIR)	http://sigir.org/sigir2019/	Annual	2019
IEEE International Conference on Data Mining (ICDM)	http://icdm2018.org/	Annual	2018
Very Large Data Bases (VLDB) conference	http://vldb.org/2019/	Annual	2019
International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT)	https://eurocrypt.iacr.org/2019/	Annual	2019
International Cryptology Conference (CRYPTO)	https://crypto.iacr.org/2018/	Annual	2019
ESORICS : European Conference on Research in Computer Security	https://esorics2018.upc.edu/	Annual	2019
ARES : International Conference on Availability, Reliability and Security	https://www.ares-conference.eu/	Annual	2019

To this end, organization of a number of special sessions in conferences have been planned; the project has already organized a special session at the 2018 GIIS conference (more details are provided at the first dissemination report D9.3).

4.3 Cyber-Trust targeted initiatives

Leading by CSCAN, UOP and KEMEA an edited volume/book will be published by well-known publishers (such as IEEE, Springer, Wiley) at the end of the project. All partners are expected to contribute in this volume/book and will be focused on IoT threat landscape and how Blockchain and Deep Packet Inspection along with Threat Intelligence and other areas considered in the project can help mitigating the attacks, promoting the work conducted in the project. It also envisioned that Cyber-Trust will organise a special issue with other projects under the same call H2020-DS-SC7-2017 (e.g. ASTRID, REACT, SPEAR) in a journal from the list of section 5.1.

Secure South West (SSW) is hosted by the Centre for Security, Communications and Network Research (CSCAN) at the University of Plymouth. SSW attracted delegates from public and private sector organisations from across the south west region. Cyber-Trust has ensured a keynote presentation during this event where Cyber-Trust partners will be present to many industry partners as well as academics and general public.

Lastly a summer school event will be organized leading by UOP, CSCAN and KEMEA as well as with other consortium partners involvement. The summer school will offer intensive training on various Cyber Security issues from both academic as well as industry partners to a mixture of people such as students, employees, and cyber-security professional in order the project to be promoted and also create a network of people and this summer school to be established as an event that will be organized yearly across Europe. We will explore the possibility to be organized under the auspices or sponsored by a variety of organizations; a minimal registration fee might be included just for covering organizational expenses and some student's stipends. Possible locations of organization could be Cyprus or Crete for this event in order to attract more people.

4.4 Workshops

Cyber-Trust recognises the utility of running workshops and attending events related to Cyber Security, as this offers a unique insight into the world of Cyber Security and offers a valuable way to cross-pollinate project ideas with other non-project ways of thinking and best practice.

By organizing or attending workshops, partners of the consortium have the opportunity to work with people of all backgrounds to share the importance of securing the Internet of Things, train people and leverage the cutting-edge research being conducted through the Cyber-Trust as well as engage those individuals whose research applies directly to the project findings.

Workshops organised alongside at international Cyber Security conferences, will allow communication of Cyber-Trust results to a wide audience, often exceeding 1,500 individuals from 60+ countries. Another way of communicating the knowledge generated in the project includes the organisation of special sessions at various broad or specialised conferences, where industrial partners are invited. All partners will be involved in the aforementioned activities in order workshops to be organized.

4.5 Synergies with Other Projects

The Cyber-Trust consortium will communicate its results to other H2020 projects working on relevant topics and consider establishing links to collaborate on aspects of mutual interest. As an example, links with the following projects will be sought during project implementation.

- ASTRID: AddreSing ThReats for virtualIseD services
- THREAT-ARREST: Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training
- REACT: REactively Defending against Advanced Cybersecurity Threats (react-h2020.eu)
- SPEAR: Secure and PrivatE smArt gRid (www.spear2020.eu)
- DEFeND: Data Governance for Supporting GDPR (www.defendproject.eu)
- BPR4GDPR: Business Process Re-engineering and functional toolkit for GDPR compliance
- PDP4E: Methods and tools for GDPR compliance through Privacy and Data Protection Engineering (www.pdp4e-project.eu)
- PAPAYA: PlAtform for PrivAcY preserving data Analytics (www.papaya-project.eu)
- SMOOTH: GDPR Compliance Cloud Platform for Micro Enterprises (smoothplatform.eu)
- OLYMPUS: Oblivious identitY Management for Private and User-friendly Services
- PoSeID-on: Protection and control of Secured Information by means of a privacy enhanced Dashboard (www.poseidon-h2020.eu)
- CYBERWISER.EU: Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training (www.cyberwiser.eu)
- ANASTACIA: Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures (www.anastacia-h2020.eu)
- PROTECTIVE: Proactive Risk Management through Improved Cyber Situational Awareness (www.protective-h2020.eu)
- SHIELD: Securing against intruders and other threats through a NFV-enabled environment (www.shield-h2020.eu)
- SISSDEN: Secure Information Sharing Sensor Delivery event Network (sissden.eu)
- DECODE: Decentralised Citizens Owned Data Ecosystem (www.decodeproject.eu)

Successful cooperation with other H2020 projects is in the interest of Cyber-Trust as it increases the scientific and economic impact of the proposed technologies. The cooperation is also expected to take the form of joint action planning, such as the organization of common workshops and events, amongst others. All partners are expected to contribute in this activity led by CSCAN, UOP and KEMEA.

5. Individual Dissemination and Communication Plan

This section details the individual communications plans as outlined by the consortium partners and in line with their capability and commitment to the project. Given the commercial sensitivities surrounding the project and its outputs, all communications activities will be overseen by CSCAN. CSCAN has the overall responsibility of the communication efforts, as being the leader of WP9. This is to provide Consortium members with the reassurance that communications will benefit the Consortium project as a whole and will not prejudice for or against individual partners.

It will also allow the consortium the opportunity to control the dissemination of information that is commercially sensitive to one or more of the partners. As stated in the project proposal, dissemination activities should not impact on the planned exploitation of the project findings, and by centralising the communication of project findings this can be more easily achieved.

CSCAN and ADITESS will form the core of the project's communication team. Together they will work continuously to keep the Cyber-Trust website updated as well as the dissemination material.

CSCAN will take the lead in liaising with individual partners regarding communications, to provide assistance with regards to confidentiality and IP, and to maintain the consistency of project communications. It will be responsible for the timing of blog posts in Cyber-Trust website, the creation of podcasts, live YouTube sessions, Linkedin posts, Facebook posts and maintaining the Cyber-Trust twitter feed. ADITESS will take the lead on the technical updating of the website, the uploading of content and the monitoring of key analytics such as web traffics statistics, subscription to RSS feeds and website email subscription numbers.

5.1 KEMEA

KEMEA's approach on dissemination and communication activities is two folded. Primarily, KEMEA aims to support and complement the Cyber-Trust consortium dissemination and communication strategy and then on individual (project beneficiary) level to define and execute its own individual dissemination and communication plans.

With regard to the overall dissemination activities of the project KEMEA will support and complement in the following activities:

- Maintain and regularly disseminate the project website and social media pages
- Organise and participate in dissemination events
- Prepare informative materials for dissemination to the media and other stakeholders in as many Member States as possible
- Prepare scientific journal articles and conference presentations
- Raise awareness among the cybersecurity community and the identified stakeholders.

In the "individual" dissemination and communication plan KEMEA will respect the consortium outreach strategy for dissemination and communication activities. KEMEA from its constitutional law and its mundus operandi, is a partner with strong relationships with end users from the LEA communities and participated in the establishment of the Greek Cybercrime Center. As such KEMEA has primarily identified the following groups which will attempt during the first year of the project to engage with them. These groups are:

1. End-Users operating in the prevention domain as a division of a LEA
2. Industry and technical experts acting in the cybersecurity industry
3. Academia with profound interest in cyber domain
4. Policy Makers at National Level
5. Related research projects

KEMEA's dissemination strategy involves a wide range of tools that will be used to disseminate the project's activities and results, and to engage with the stakeholders mentioned above. These tools are shown in **Error! Reference source not found.**.

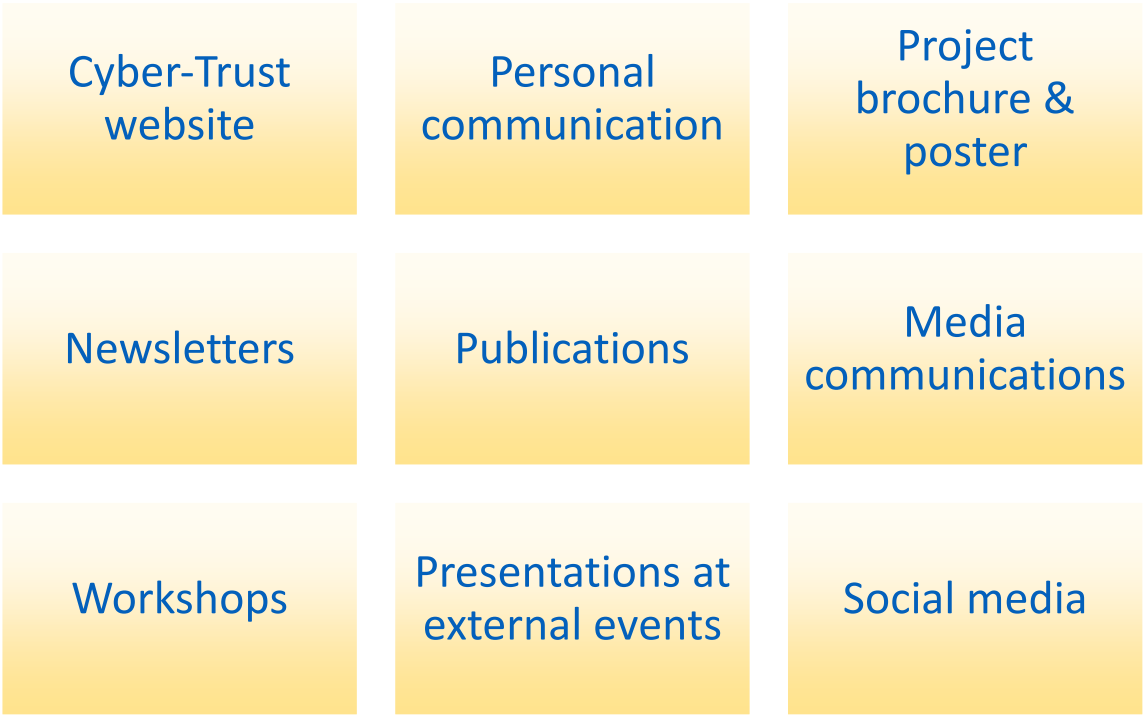


Figure 5.1: Dissemination and communication tools

KEMEA is planning to gradually utilize the above tools (as soon as they will become available) in the initial engagement with the identified five (5) groups stated above. It is expected that each tool will have a different impact and effectiveness in engaging with each of the diverse target stakeholder groups. Initially KEMEA will promote the Cyber-Trust project in its affiliated LEA network and the internal divisions of the Hellenic Police who had expressed an interest in Cyber-Trust project and are involved in Cyber Security. Later, in 2019 when the project will produce tangible result, KEMEA will start propagating the project outcomes within its professional network. The plan is to have an ongoing engagement strategy utilizing project brochures, newsletters, social media and presentations when they become available and disseminate information to its target stakeholders and maintain their interest in the project's scope.

5.2 UOP

As a higher education establishment UOP aims primarily at communication and dissemination activities targeting the RTD community and the academia at large. The main dissemination and communication target audience for the project and its results is mainly the Cyber Security research community, encompassing researchers, scientists and students with interests similar to the Cyber-Trust research topics. However, the communication of the projects' results and distribution of information will also aim at wider audiences such as the broader scientific RTD community, European commercial and industrial stakeholders, as well as other EU-funded and national projects, that will be interested in and benefit from the project's outcomes.

To do so, all appropriate channels will be utilized; communication of the project itself will be facilitated to the target audiences mainly through invited talks in partner institutions and invited publications in relevant venues. Indicatively:

Table 5.1: Target group and communication instruments

Target group	Communication instruments
▪ Cyber Security researchers ▪ Academia and RTD centres	▪ Scientific publications ▪ Seminars/training sessions
▪ IT professionals ▪ Commercial and Industrial stakeholders	▪ Open days/summit/events ▪ Seminars/training sessions
▪ Other research projects	▪ Joint dissemination activities

To maximize the penetration and impact of the dissemination activity, communication of the project and its results will be adapted (e.g., in terms of terminology, presentation of details, etc.) to fit the background and interests of its target audience. Communication of the project's results will be mainly achieved through publications in high-impact journals and magazines, conferences, and specialized workshops pertaining the project's research topics.

In particular, during the first period of the project, the planned dissemination activities of UOP aim to foster research collaboration opportunities along with clustering activities with other projects, exchange knowledge, and raise awareness of Cyber-Trust's research areas: in cyber-threat intelligence gathering and sharing techniques, trust management and risk/vulnerability assessment, game-theoretic security and intelligent cyber-defense, cryptographic and other security mechanisms for privacy, blockchain architectures and with an emphasis on securing the IoT. Hence, the target audiences, as per the above table, will mainly be Cyber Security researchers, researchers at large, academic institutions and RTD centres. The main goal is to achieve at least six publications during the first half of the project, and at least three invited talks to be given at academia/RTD centres or other events. In addition, the organisation of two special sessions or workshops are envisioned that are related to the above areas.

Dissemination activities are expected to be more intense during the second period of the project, since it is expected that the project will have achieved more mature results than in the first phase. As tangible technical results are expected to be available, this will provide the ground to offer a wider dissemination of Cyber-Trust in the scientific community, but to also include IT professionals as well as European Commercial and Industrial stakeholders. During the second half of Cyber-Trust, will:

- Seek to publish Cyber-Trust results in high-quality conferences and international scientific journals and present the project outcomes at a major academic conference, discussing the project ideas and results with the academic and industrial community attending the event.
- Continue seeking clustering opportunities with other EU-funded projects (see e.g. the list provided in Section 4.5) to increase collaboration and organize joint workshops (at least one is foreseen) at major Cyber Security related events.

Overall, throughout the project, based on the progress and achievements, UOP will seek suitable venues for publishing the scientific results of the project, with special emphasis on its major areas of expertise: security, cryptography, privacy and trust, information retrieval, data management, game theory, and distributed systems.

5.3 CGI

CGI is one of the largest IT and business process services providers in the world. As a large industry representative, CGI’s dissemination and communication strategy and activities of the Cyber-Trust project will be targeting towards its clients on different industries ranging from defence and intelligence to educational and research organisations. CGI’s main dissemination and communication target audience for the Cyber-Trust project will be law enforcement, security and defense clients as a first priority since the project output is expected to have validated pilot, then all other industries which will benefit from the project. Considering the key role of CGI in the project (leading solution architecture practice) CGI will disseminate and communicate the project progress activities and results in the area of architecture in Cyber-Trust. In particular, applying RCDA (Risk and Cost Driven Architecture methodology) in practice on designing modular architecture of the Cyber-Trust system comprising the main tools: 1) Cyber-Trust proactive technology tools, 2) Cyber-Trust attack detection and mitigation tools; 3) Cyber-Trust distributed ledger technology tools.

CGI is also a co-founder of the Open Innovation 2.0 within the European Commission's OISPG (Open Innovation Strategy and Policy Group), where the collaboration and co-creation among multidisciplinary stakeholders is essential, CGI will also disseminate and communicate the project's activates, status and results using the OISPG network aiming at multiplier effect.

During the first year of the project, the dissemination and communication actvivites will be mainly focusing on awareness raising of Cyber-Trust project and informing on the development and the status. The second year will be a combination of awareness raising and disseminating on the interim outcomes of the project. The last year will build upon the previous years' activities and mainly focus on communicating and disseminating the project's status and outcomes.

As means of communication and dissemination, CGI plans to write blogs and publish papers (scientific and business) individually and in collaboration with relevant project partners reflecting the work performed. CGI will share the news items and the project's publications, blogs using company's intranet (reaching out 73000 members), CynerGI internal CGI communication platform targeting specific focus expert communities (IoT, cybersecurity, blockchain), CGI's official Linked-In page and Twitter. CGI will also use any opportunity to disseminate and communicate project's actvities and results in relevant events, such as conferences, exhibitions, workshops and focused subject matter meetings.

This plan will be regularly reviewed and if needed updated based on the priorities of the project and the European Commission, the current project's results achieved and any new measures set.

5.4 MATHEMA

Mathema is a small company from Florence (ITALY) with a long experience in designing and deploying advanced IT solutions for private and public (e.g. Italian Ministry of Foreign Affairs) customers. In order to raise the awareness about the importance of Cyber Security in IT systems especially within the IoT domain.

MATH dissemination activities will be mainly organised in:

- organising small meetings within its network of customers and security experts to communicate the advances in research stemming from Cyber-Trust activities and exploring the industrial perspectives of application in its market
- organising joint events with its long-term research partners (e.g. University of Florence and Italian National Council of Research) to discuss further potential improvement and promote the technology transfer in the field, also actively involving young researchers in this field
- giving evidence of project's main achievements through its web site (www.mathema.com) and other social media

Mainly starting from the second year of activities:

- joining other partners in large events (both industrial and scientific conferences) to present project's outcomes
- collaborating to papers and other scientific dissemination

Moreover, thanks to an invited visiting period of a member of the company (dr. Emanuele Bellini), a special connection will be established with the Cyber Security Centre at Khalifa University of Abu Dhabi. In particular, will be disseminated the topics and the results of Cyber Trust project and in turn we learn the state of the art of their current research results. Finally, Cyber-Trust and Khalifa University joint or co-sponsored events can be organised on the cyber security topics.

5.5 MTN

MTN is the largest private telecommunication company in Cyprus, with the focus always being at providing high quality services towards its customers. With the evolution of IoT in the following years the uptake of Smart Home appliances by consumers and M2M communication overall is to be increased. The importance, therefore for security and overall safety while using smart devices becomes essential. MTN will effectively contribute to the dissemination of the Cyber-Trust results and the importance of the solution being in place overall in an ISP environment, to create awareness around the essence of the IoT security and safe use as well as to communicate the significant information and services that an ISP can provide to the end users. Main activities to be held from MTN include publishing press releases related to the project itself as well as its results, as well as blog posts in the company's blog and social media campaigns targeting its customers and businesses across.

5.6 VUB

VUB plans to contribute effectively to the communication and dissemination of the project and its findings, focusing in particular on the key output of WP3 which VUB leads, by engaging in various activities and events. Specifically, VUB in cooperation with the interdisciplinary Research Group on Law Science Technology & Society as well as the Brussels Privacy Hub and other partners aims to organise at least one relevant workshop/conference/talk/master class per year. The targeted audience of those activities ranges from the general public to academia representatives, legal scholars, cybersecurity experts and policy makers. In parallel, VUB aims to register at least three talks and panels at well-established in the field events and conferences, such as the Computers, Privacy and Data Protection Conference (CPDP), the Annual Privacy Forum and the Brussels Privacy Symposium. As academic partner, VUB intends to produce at least two high-quality peered and non-peered review publications for academic journals and scientific magazines, for instance, the European Data Protection Law Review, the International Data Privacy Law and the Stanford Journal of Blockchain Law & Policy. VUB also aims to raise awareness by contributing with its gained expertise to relevant working groups, advisory boards and experts´ fora. The relevance of all these activities to Cyber-Trust would range from medium to high. The following overview is indicative, as more activities are envisaged to be organised along the way.

5.7 SCORECHAIN

As a Regtech startup, Scorechain aims primarily at communication and dissemination activities targeting, financial and IT professionals, cybercrime professionals, law enforcement agencies and researchers. Any person related to Cyber Security might be interested in our outputs due to the problems and solutions we encountered during the project. We often travel to present our Blockchain monitoring products so it will be an opportunity to highlight Cyber-Trust project as well.

Different channels will be used to communicate to the possible target audience.

Table 5.2: Target group and communication instruments

Target of audience	**Communication instruments**
Cyber Security researchers Students	Seminars/conferences/training sessions/international fairs
IT, financial professionals, cybercrime	Social networks, newsletters/international fairs
Law enforcement agencies	Meetings, newsletters

Of course, the vocabulary will be adapted to the situation and the public attending the event. Our two founders are serial public speakers for international conferences and seminars with audience from different background.

During the first year of the project, we plan to raise awareness about our participation to the project and the issues it aims to resolve. The second year, we will communicate about the technological choice and capabilities we made during the early development stage of the project. Finally, during the last year of the project we will communicate about the results of the development and doing some demonstration of a beta version of the software running.

Overall our communication about the project will be oriented around the blockchain and cryptocurrency space. We will adapt our speech and communication channels to impact Cyber-Trust targets. E.g. Why is blockchain suitable for Cyber-Trust? What will be the advantages of using a blockchain? What is the power of Blockchain transparency and immutability for monitoring cyber threats?

5.8 ADITESS

ADITESS dissemination activities will focus on contributions at the preparation of papers targeting international conferences and journals as well as **c**ontributions on the continuous content update of the Cyber-Trust Project website, Cyber-Trust Social Media content as well as content on other dissemination channels. Moreover, ADITESS will look for any opportunities to propose articles and news on newsletters and mailing lists of organizations in which ADITESS is a member, or in any case focused on the Cyber-Trust topic. Newsletters, brochure, and other project dissemination materials will be distributed via on-line channels taking advantage of ADITESS established contacts at local and International level. ADITESS will also disseminate printed version of brochures, newsletters on conferences, workshops, meetings with subjects potentially interested on Cyber-Trust.

Further, ADITESS will have several meetings with potential end-users at local level in order to create a target group interested in the project development, and to receive relevant feedback. Such meetings will be held anytime a potential stakeholder will be contacted in the future.

Linking activities with related projects will focus on the European Enterprise Network Cyprus (www.bsccyprus.org.cy part of www.een.ec.europa.eu).

The below target groups and actions is a combination of communication, dissemination and exploitation actions:

- Meeting with Research Promotion Foundation http://research.org.cy in order to introduce the Cyber-Trust project and future use of EEN platform (that RPF coordinate in Cyprus) for dissemination of outputs as well as help on exploitation and commercialization of the product/service /output of the project. Founded in 1996, the Research Promotion Foundation (RPF) was established at the initiative of the Government of the Republic of Cyprus, to promote the development of scientific and technological research in Cyprus due to the fundamental importance of research in contemporary societies. The Foundation's core objective is the promotion of scientific and technological research in Cyprus. Several specific objectives and priorities have been defined by the Foundation's Statute and the decisions of its Board of Directors, for the promotion of this main objective.
- Meeting with Cyprus Telecommunications Authority. CYTA has shown a preliminary interest but also an intention of collaboration with ADITESS, as regards the latest technology projects that ADITESS is involved.
- Academic Community:
    - University of Cyprus. A preliminary interest in collaborating was showed by KIOS Research Center for Intelligent Systems and Networks that operates within the University of Cyprus. Through the continuous communication with KIOS potential further collaboration may come up in future.

- European University Cyprus. A potential close collaboration with the Engineering School can be reached in order to further exploit the Cyber-Trust outputs.

5.9 CSCAN

The Centre for Security, Communications and Network Research (CSCAN) is an established research group, comprising staff from the School of Computing, Electronics and Mathematics at the University of Plymouth. University of Plymouth is a non-profit educational and research organisation as such does not aim for generate profit. However, the Cyber-Trust outcomes, particularly those leading to high quality and high-impact publications by CSCAN staff, will be considered for submission to the UK Research Excellence Framework (REF) in 2020. REF is the evaluation mechanism used by the UK government for allocating research funding to UK research organisations, and as such contributes to the economic viability of the University of Plymouth.

During the first year of the project CSCAN will:

- Seek to publish Cyber-Trust results in IT Security professional magazines in UK and EU such as ITNOW.
- Promote Cyber-Trust project through the University of Plymouth media office press.
- Promote Cyber-Trust during Open Days and Applicant Days

During the second year of Cyber-Trust, CSCAN will:

- Seek to publish Cyber-Trust results in high-quality conferences and international scientific journals and present the project outcomes at a major academic conference, discussing the project ideas and results with the academic and industrial community attending the event.
- Continue seeking clustering opportunities with other EU-funded projects (such as the ones on the list in Section 4.5) to increase collaboration and organize joint workshops (at least one is foreseen)
- Promote Cyber-Trust at Secure South West – SSW (regional security dissemination event organised by CSCAN) through a keynote presentation and reach UK/EU industry as well as researchers.

Overall, throughout the project lifespan, CSCAN will identify and target suitable venues for publishing the scientific results of the project, with special emphasis on its major areas of expertise: Cyber Security, Deep Packet Inspection, Network Anomaly Detection, Malware mitigation and Botnet mitigation.

6. Key Performance Indicators

Measuring the success of Cyber-Trust's dissemination activities is crucial to the success of the project, and this will be done using a variety of metrics.

Direct engagement will be measured by looking at website traffic statistics, and an interrogation of that data will help the consortium to analyse which tools are better than others at reaching a broad audience. Social Media engagement can be used to ascertain how many individuals and organisations are interacting with Cyber-Trusts content at any one time.

For more complex tools such as speaking engagements at conferences, workshops and taught courses, we can use attendee numbers, short questionnaires, and external validation exercises to assess the success of each event.

All this will be conducted in an effort to continually review which tools work, which don't, and how we can improve communications going forward. With this continual improvement in mind it, CSCAN, as part of its project deliverables, will produce a yearly report looking into the dissemination activities of the Consortium partners and assessing what, if any, changes need to be made to the dissemination plan.

Table 6.1: Cyber-Trust KPIs

Dissemination tool/channel	KPI	Objective	Targeted Audience						
			European Commercial & Industrial stakeholders	ISPs	LEAs & Governmental agencies	Research Community	Projects	EU citizens	IT professionals
Website	Visits	300 per month	√	√	√	√	√	√	√
Brochures	Number produced	3	√	√	√	√	√	√	√
Scientific Publications	Number of publications	15	√		√	√	√		√
Press Releases	Number of publications	8	√	√	√	√	√	√	√
Blog	Number	10	√	√	√	√	√	√	√
Newsletter	Number	5	√	√	√	√	√	√	√

Workshops	Number	At least 5	√	√	√	√	√		√
Presentations at Events	Number	30	√	√	√	√	√	√	√
Social Media	Number of Likes, Retweets	At least 40	√	√	√	√	√	√	√
Direct Contact			√	√	√	√	√		√

7. Advisory Group

The Advisory Board (AB) has been established from the very beginning of the project, with the aim to facilitate cooperation with the relevant stakeholders. The Cyber-Trust AB is led by Cyber Security experts that will undertake advisory and consulting activities regarding IoT & Smart Home/City, DLT and digital forensics, providing additional expertise.

The role of the AB is to provide their advices and guidance as end-users and industrial partners ensuring that the Cyber-Trust solution and results will be practical and of added value for the end-users. To this extend, the AB will also evaluate the project’s findings and outcomes and provide consultation to the General Assembly. The AB will be supervised by the project Coordinator and WP9 Leader. They will attend five AB meetings during the three years of the project, in which Cyber-Trust partners will present the status of the project, their research activities and results as well as their development plans.

Table 7.1: Cyber-Trust AB

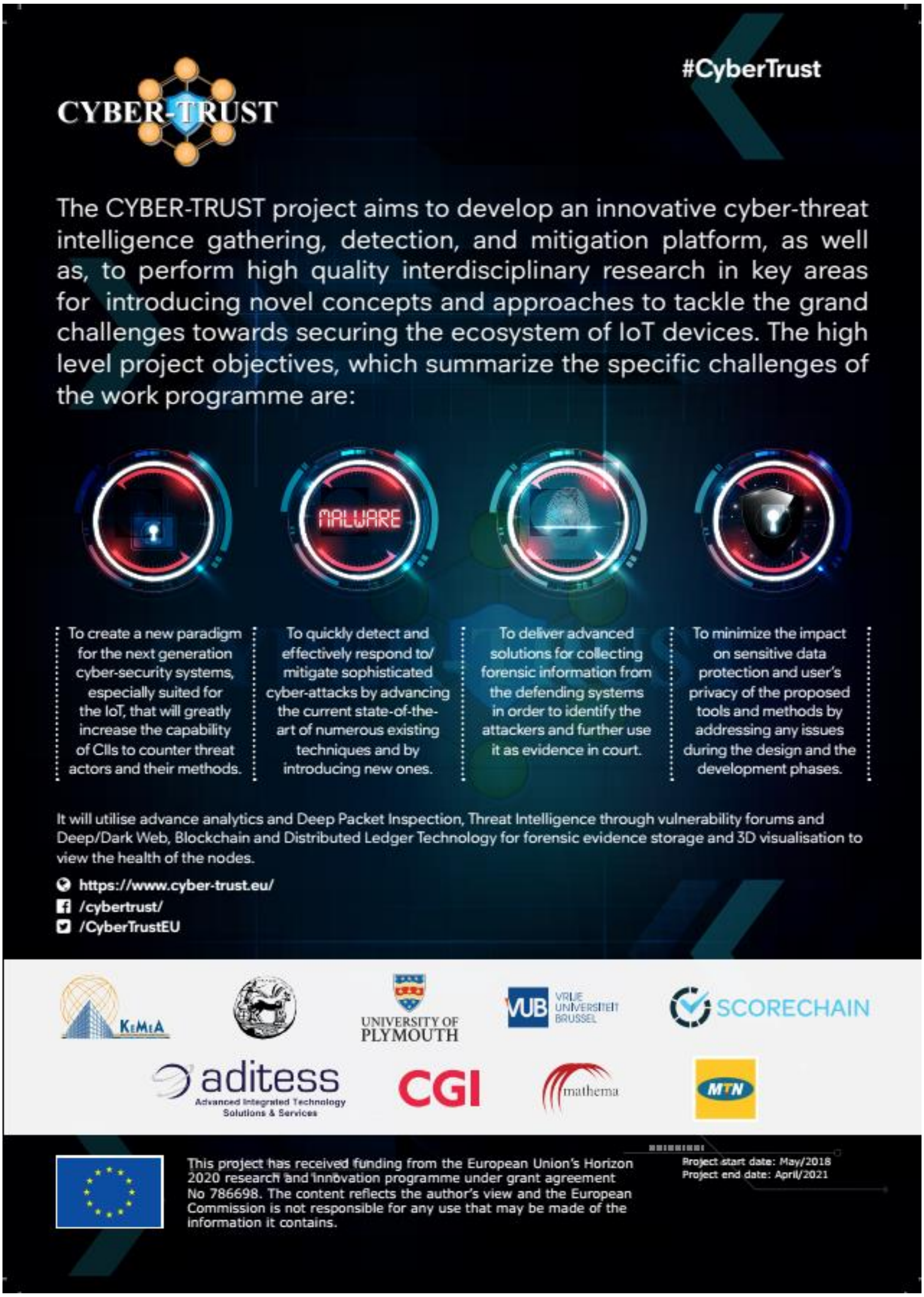
AB member	Affiliation	Country	Expertise
Mary-Jo de Leeuw	Associate partner Cyber Security & innovation at Revnext; President General Board of Cyberwerkplaats foundation; President of Platform Internet of Toys; Vice president of Women in Cyber Security Foundation	Netherlands	Cyber Security, Internet of Toys, Internet of Things, Wireless communication
Roberto Gavazzi	Smart City and Industrial Internet Senior Program Manager at TIM	Italy	Internet of Things, Industrial internet, Smart Cities

Konstantinos Papapanagiotou	Leader of Open Web Appl. Security Project (OWASP) Greek Chapter	Greece	Information Security
Matteo Maffei	Head of Security and Privacy Group of TU Wien	Austria	Cryptographic protocols for the security and privacy of cryptocurrencies, cloud services, and analytics
Athanasios Lioumpas	Cyta Hellas Telecommunications Engineer & Senior Researcher	Greece	Electronics and communication engineering. Wireless communications and networks
Vasilis Katos	Bournemouth University: Head of Computing and Informatics	UK	Cybersecurity, Digital Forensics
Paul A. Galwas	Security Architect of the Digital Catapult, Crossword's Chief Scientific Officer	UK	Security technologies, Cryptography, Security architectures
Geleyn R. Meijer	Rector of Amsterdam University of Applied Sciences	Netherlands	Internet of things, Smart Cities, Creative Industries, Digital Media and Digital Security

8. Conclusion

This document outlines the Dissemination Plan for the Cyber-Trust Project and will serve as the principle communications guide to how the project will disseminate findings and research to the target audience to raise its present. The exploitation plan of the project will be introduced in deliverable D9.9 at M12 where partners will also explore the potential commercialization of Cyber-Trust. During the next period of the project this plan will be followed in order project to meet its goal and achieve higher visibility and recognition from both industry and academia.

Annex A – Cyber-Trust Flyer



#CyberTrust

CYBER-TRUST

The CYBER-TRUST project aims to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform, as well as, to perform high quality interdisciplinary research in key areas for introducing novel concepts and approaches to tackle the grand challenges towards securing the ecosystem of IoT devices. The high level project objectives, which summarize the specific challenges of the work programme are:

To create a new paradigm for the next generation cyber-security systems, especially suited for the IoT, that will greatly increase the capability of CIIs to counter threat actors and their methods.

To quickly detect and effectively respond to/ mitigate sophisticated cyber-attacks by advancing the current state-of-the-art of numerous existing techniques and by introducing new ones.

To deliver advanced solutions for collecting forensic information from the defending systems in order to identify the attackers and further use it as evidence in court.

To minimize the impact on sensitive data protection and user's privacy of the proposed tools and methods by addressing any issues during the design and the development phases.

It will utilise advance analytics and Deep Packet Inspection, Threat Intelligence through vulnerability forums and Deep/Dark Web, Blockchain and Distributed Ledger Technology for forensic evidence storage and 3D visualisation to view the health of the nodes.

https://www.cyber-trust.eu/
/cybertrust/
/CyberTrustEU

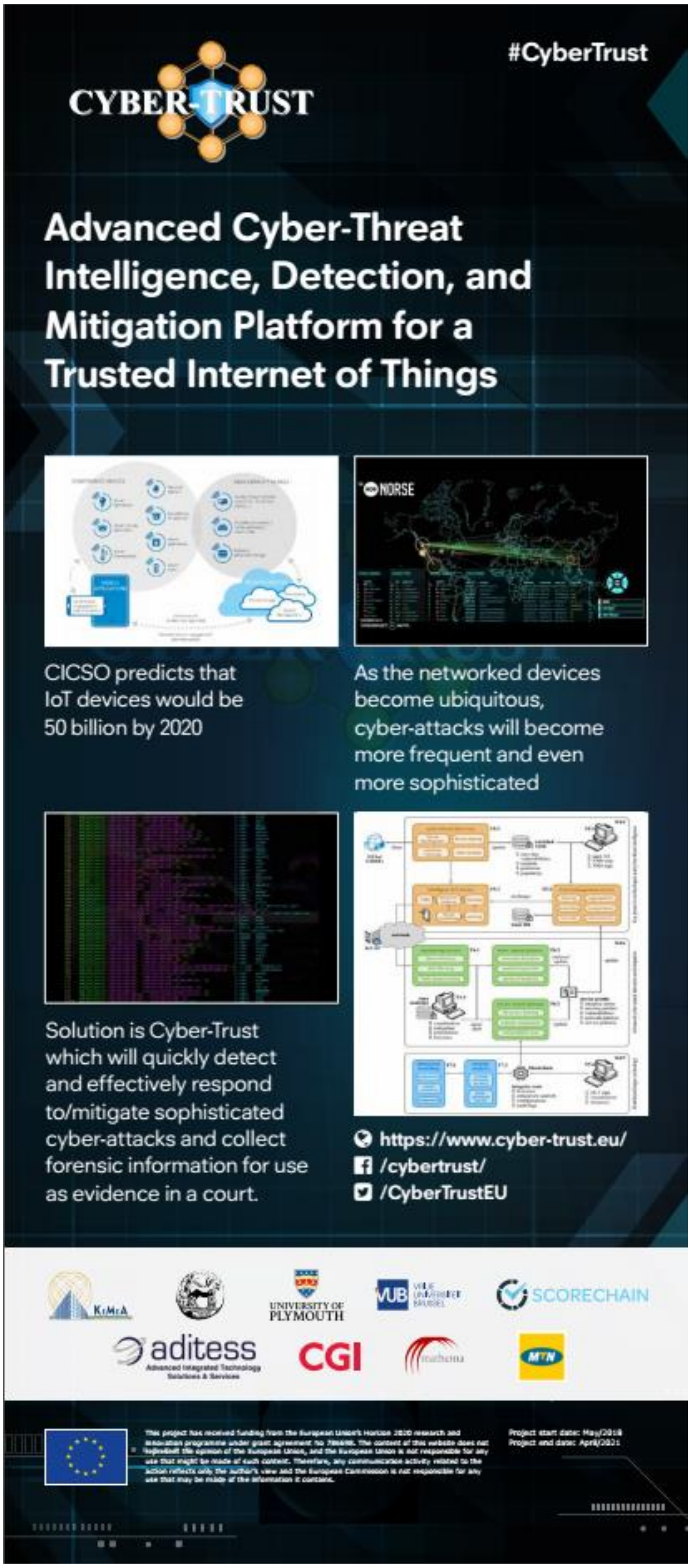
KEMEA
UNIVERSITY OF PLYMOUTH
VUB VRIJE UNIVERSITEIT BRUSSEL
SCORECHAIN
aditess Advanced Integrated Technology Solutions & Services
CGI
mathema
MTN

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. The content reflects the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Project start date: May/2018
Project end date: April/2021

Figure A.1: Flyer

Annex B - Cyber-Trust Banner



#CyberTrust

CYBER-TRUST

Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things

CICSO predicts that IoT devices would be 50 billion by 2020

As the networked devices become ubiquitous, cyber-attacks will become more frequent and even more sophisticated

Solution is Cyber-Trust which will quickly detect and effectively respond to/mitigate sophisticated cyber-attacks and collect forensic information for use as evidence in a court.

https://www.cyber-trust.eu/
/cybertrust/
/CyberTrustEU

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. The content of this website does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content. Therefore, any communication activity related to the action reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Project start date: May/2018
Project end date: April/2021

Figure B.1: Poster

Annex C – Dissemination information gathering document (to be based on the templates of the project periodic report)

Table C.1: Dissemination Report Activity Table

Date	
Communication Activity	
Communication Type	
Target Audience (Please Circle One or More)	Partners General Academic Government Industry
Partner Involved	
People Involved	
Description of the activity, relevance to the Project and Impact	
Link to material	
Photo of attendance	