Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: February 1, 2019
Project duration: 42 months

Cyber Security for Europe

D9.5

Report on the Outreach and Dissemination Activities 1

Document Identification	
Due date	31 January 2020
Submission date	31 January 2020
Revision	2.00 (24 July 2020)

Related WP	WP9	Dissemination Level	PU
Lead Participant	UMA	Lead Author	Carmen Fernandez-Gago, Javier Lopez (UMA)
Contributing Beneficiaries	TDL, UMA	Related Deliverables	D9.3, D9.4, D9.7, D10.1

Abstract: This document describes the outreach activities, that is, the dissemination and communication activities carried out by the CyberSec4Europe partners during the first year of the project. These activities are in alignment with the Dissemination and Awareness Plan of the project.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under Grant Agreement no. 830929. This document and its content are the property of the CyberSec4Europe consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or licence on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe partners. Each CyberSec4Europe partner may use this document in conformity with the provisions of the CyberSec4Europe Grant Agreement and Consortium Agreement.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

This is an annual deliverable on the outreach activities of all CyberSec4Europe partners and is one of a series of deliverables that demonstrate how the project objectives and results are communicated to its target audiences. This document is the first report in this series providing details of the dissemination and communication activities of CyberSec4Europe during its first year. These activities follow the project strategy for communication and dissemination, designed at month six. Thus, as the strategy plan identifies different target audiences and different dissemination and communication channels, this document aligns with that classification in order to provide a detailed picture of the activities carried out.

Document information

Contributors

Name	Partner
Carmen Fernandez-Gago	UMA
Javier Lopez	UMA
David Goodman	TDL

Reviewers

Name	Partner
Stephan Krenn	AIT
Dmitry Pap	ATOS
Ahad Niknia	GUF
Narges Arastouei	GUF
David Goodman	TDL

History

0.01	2020-01-22	Carmen Fernandez-Gago	1st Draft
0.02	2020-01-23	Carmen Fernandez-Gago Javier Lopez	Comments by AIT, GUF and ATOS addressed
0.03	2020-01-27	Carmen Fernandez-Gago Javier Lopez	Dissemination activities by GUF
0.04	2020-01-27	Carmen Fernandez-Gago Javier Lopez	Section 5 included on joint activities with the other pilots
0.05	2020-01-29	Carmen Fernandez-Gago Javier Lopez	Submitted for final high-level review to reviewers
0.06	2020-01-30	Ahad Niknia	High-level review
Final	2020-01-30	Carmen Fernandez-Gago Javier Lopez	Final version ready for submission
1. 1	2020-06-16	Carmen Fernandez-Gago Javier Lopez	Comments made by the reviewers for the first period report addressed

1. 2	2020-07-17	Carmen Fernandez-Gago Javier Lopez	Comments made by David Goodman addressed on version 1.1
1.3	2020-07-23	David Goodman	Cosmetic comments on version 1.2
2.0	2020-07-24	Carmen Fernandez-Gago	Final version ready for re-submission

List of Contents

List of Figures

List of Tables

List of Acronyms

AIT	Austrian Institute of Technology GmbH
B2B	Business to Business
CANVAS	Constructing an Alliance for Value-driven Cybersecurity
CNR	National Research Council (Consiglio Nazionale delle Ricerche)
CODE	Research Institute of Cyber Defence (translation to English from German)
COMPACT	Cybersecurity for Public Administrations
CONCORDIA	Cybersecurity Competence for Research and Innovation
CyberSec4Europe	Cyber Security for Europe
CYBER	Cybernetica
DG CNECT	Directorate-General for Communications Networks, Content and Technology
DG HOME	Directorate-General for Migration and Home Affairs
DIN	German Institute of Standardization (translation to English from German)
DTU	Technical University of Denmark
ECHO	European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations
ECSO	European Cyber Security Organisation
EU	European Union
GUF	Goethe University Frankfurt
JAMK	Jyvaskylan Ammattikorkeakoulu
JRC	Joint Research Centre
KAU	Karlstadt University
KPI	Key Performance Indicators
MEP	Member of European Parliament
NIA	Information Technology and Applications (translation to English from German)
NeCS	Network on CyberSecurity
OASC	Open &Agile Smart Cities
REA	Research Executive Agency
SDO	Standards Developing Organisation
SPARTA	Strategic Programs for Advanced Research and Technology in Europe
TU Delft	Technical University of Delft
UCY	University of Cyprus
UMA	University of Malaga
UMU	University of Murcia
UNITN	University of Trento
VTT	Teknologian tutkimuskeskus VTT Oy
WG	Working Group

1 Introduction

The creation of the Digital Single Market has been one of the key goals of the EU for many years. This means that new security challenges arising in this context need to be tackled, considering different perspectives. One of these perspectives is the coordination among experts to work together effectively in order to be able to anticipate failures of systems or malicious attacks. This is the context of the project. Thus, the main objective of CyberSec4Europe is to create a coordinated network of experts in the field of cybersecurity that are able to determine the best practices needed in order to respond to failures or attacks that would hamper the development of a Digital Single Market.

CyberSec4Europe is, together with CONCORDIA, ECHO and SPARTA, working towards this objective that will be the seed for the creation of a cybersecurity competence network with a European Cybersecurity Research and Competence Centre.

Given the importance of the key objectives of CyberSec4Europe, it is of paramount importance how its partners communicate how the project's research and innovation will deliver results and account for public spending as well as to demonstrate that its research achieves scientific excellence and helps solve societal challenges. It must explain to the citizens of Europe how the outcomes of its work are relevant to their everyday lives, through improving their security and economic well-being. The project must spread its results so that policy makers are better informed and that the rest of the scientific community and industry can benefit from this work.

According to [D9.3] the benefits of effective dissemination and awareness are the ability to:

- draw the attention of national and regional governments, and potentially other public and private funding sources, to the work of the pilot;
- attract the interest of potential partners;
- attract first rate students and scientists to join the partners' institutes and enterprises;
- enhance the standing and visibility of the partners, both at a national and international level;
- assist with the search for financial backers to exploit results.

Thus, in order to achieve the effective communication mentioned above in a successful manner, the project's dissemination and awareness strategy identified an appropriate set of target audiences which are: social, technical, scientific, business, legislative and standardisation bodies.

([D9.3]) also identified the main communication and dissemination channels that are to be used to reach these target audiences.

In this deliverable we have followed the classification in audience categories given above for listing details of all the communication activities that have been carried out, specifying the main channel used for each.

We have compared the achievements on dissemination and communication with the key performance indicators established in the strategy document as indicators of success and have stated that, for most of the KPIs, CyberSec4Europe is working well in advance of what is expected at this stage of the project.

Thus, the structure of this deliverable is as follows. Section 2 summarises the dissemination and awareness plan delivered in [D9.3]. This plan includes the target audiences that are identified in order to build the outreach activities and it is this classification that we include in Section 3 to describe these activities. In

Section 4 we compare the achievements of CyberSec4Europe against the KPIs in [D9.3]. This analysis shows us that the work done by the partners during the first period is well ahead of what is expected at this stage during the rest of the project. Section 5 describes the activities that have been carried out done in collaboration with the other three pilots and Section 6 provides our conclusions.

2 Dissemination and Awareness Plan

[D9.3] provides the details of the narrative for CyberSec4Europe and the target audiences for the project in terms of dissemination and communication. These include the details for the most appropriate channels to reach these groups and the methodologies to best achieve awareness.

2.1 Target Audiences

The potential audiences for CyberSec4Europe are extremely varied and diverse, each with its own characteristics, associated perspectives and messages pertaining to cybersecurity. They have been identified in different categories as we can see in Figure 1. For each of these audiences the dissemination and awareness plan identifies a different and appropriate communication channel.

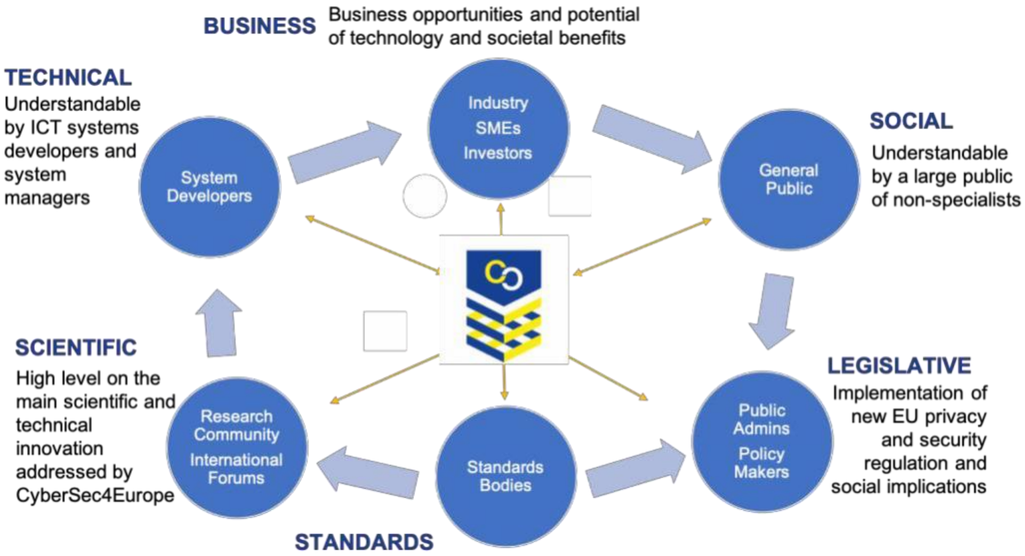

BUSINESS
Business opportunities and potential of technology and societal benefits
Industry
SMEs
Investors
TECHNICAL
Understandable by ICT systems developers and system managers
System Developers
SOCIAL
Understandable by a large public of non-specialists
General Public
SCIENTIFIC
High level on the main scientific and technical innovation addressed by CyberSec4Europe
Research Community
International Forums
LEGISLATIVE
Implementation of new EU privacy and security regulation and social implications
Public Admins
Policy Makers
Standards Bodies
STANDARDS

Figure 1 : Target Audiences

Table 1 contains a summary of these channels and their targeted audience.

Target Audiences	Potential Users	Technical level	Main focus	Medium
Social	General public Public administrations	Understandable by a large public of non-specialists	Economic impact and benefits to society and individuals Personal data protection and software security awareness and measures.	General project presentation
Technical	System developers	Understandable by ICT developers, testers, system managers and auditors	Software development cycle and end-user requirements.	Specific project presentation
Scientific	Research community International forums	High level on the main scientific and technical innovation addressed by CyberSec4Europe	Scientific innovation	Technological presentations Journal articles and conference papers
Business	Industry SMEs Investors	Business opportunities and potential of technology and societal benefits	Scientific and technical innovations. Business opportunities identification;	Business-oriented project presentation.
Legislative	Public admins Policy-making	Legislative and social implications; potential background for high-level strategic decisions	Implementation of the new EU privacy and security legislation and cybersecurity strategy.	
Standard-isation	SDOs	Standards development	Development of standards addressing cybersecurity aspects	Collaboration in standardization activities.

Table 1: Target Audiences, Messages and Channels

In this deliverable (see Section 3) we will report on how this communication plan has been achieved.

2.2 Channels for Dissemination and Communication

Communication and dissemination are clearly defined by the European Commission as two separate but interrelated approaches. In order to fulfil the objectives of CyberSec4Europe we identified in [D9.3] the following channels (Figure 2). These channels are the main means used for passing the message to the targeted audiences mentioned above. They are:

Communication

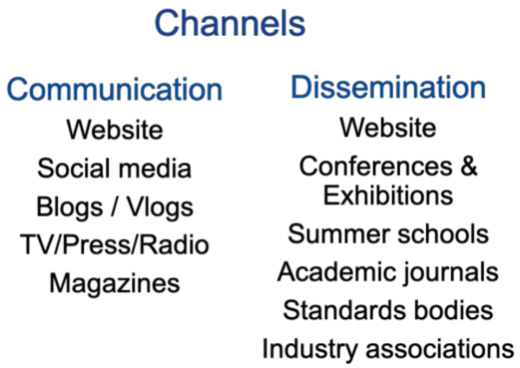
The communication channels identified for CyberSec4Europe are diverse and are mainly used for communicating with the general public. Thus, the website is the main channel of communication and presentation of the project comprising blogs on specific topics and developments of the project. Undoubtedly, press releases are also an important way to reach a general audience.

Dissemination

Dissemination aims to take the project's messages to more specialised audiences. Thus, one of the main target audiences is the scientific community. The main dissemination channels for them are scientific publications and the participation and organisation of conferences, workshops and exhibitions.

Also, stakeholders are a group target audience and they will be mainly reached by approaching their corresponding industry associations or standard bodies.

To fulfill the objectives of CyberSec4Europe identified in [D9.3] the channels seen in Figure 2 are the main means of reaching out to the targeted audiences mentioned above:



Channels

Communication
Website
Social media
Blogs / Vlogs
TV/Press/Radio
Magazines

Dissemination
Website
Conferences & Exhibitions
Summer schools
Academic journals
Standards bodies
Industry associations

Figure 2 : Channels for Dissemination and Communication

3 Dissemination and Outreach Performed Activities

In this section we describe how the target audiences that we stated in Table 1 have been approached by the consortium partners. We specify for each of these events the communication channel that was used.

3.1 Social

The results and objectives of CyberSec4Europe are communicated to the general public are generally carried out through the website, press releases or open events and exhibitions. Figures and details on the website and press releases can be found in [D9.3].

- Javier Lopez (UMA) participated in a breakfast organised by the local newspaper from Malaga (Diario Sur) in January 2020 about threats and new challenges for cybersecurity. The event was broadcast through the newspaper’s website. It was an informal discussion where the representative from UMA explained the approach of CyberSec4Europe in the European framework.
- CNR included an article in the newspaper Il Sole 24 Ore describing CyberSec4Europe and their role in the project. The article was released in November 2019.
- OASC presented the project and its importance for smart cities at SynchroniCity scale-up meeting, Milan, October 2019.
- The project was presented during the European Researchers' Night by UCY in Nicosia on the 27 September 2019. The European Researchers’ Night is an event organised by the European Commission to make all European citizens aware of the work that is being done with European funding, specially focused specifically but not exclusively to Marie Curie funding projects.
- Open Expo Europe. Madrid, July 2019. This event is an opportunity to establish contacts with possible stakeholders, meet new partners and learn more about future trends within the IT sector and the latest innovations. ATOS attended this event where they informed about the latest project news and shared some project flyers.
- Digital Enlightenment Forum/Trust in Digital Life, Brussels, July 2019. Presentation by AIT on “Privacy-preserving self-sovereign identity management” (results from WP5) at the “Towards Trustworthy Digital Identities in Europe” workshop.
- Workshop on “Cybersecurity solutions for Local Public Administration”, 14 June 2019, Venice organised by ENG’s Research & Innovation Department. The workshop was a great opportunity to show important issues in cybersecurity to an audience with very important needs and facing specific challenges to becoming cyber-resilient.
- Members of GUF were interviewed on radio in Hessen public info radio (rotation). The interview took place in March 2019 and the podcast is available online.
- A TV report was broadcast on Hessen public TV prime time and late evening TV to announce the launch of the project in February 2019. GUF was responsible for promoting this video.
- All the partners disseminated the launch of CyberSec4Europe in press releases in local or national newspapers. A report is available in D9.1.

3.2 Technical

In this audience group we include stakeholders and system developers, who are more interested in the practical aspects of CyberSec4Europe and its potential benefits as end users of the technology provided by the project.

- OASC participated in the annual meeting of the Global Digital Innovation Alliance organised at the Smart City Expo World Congress 2019 held in Barcelona, November 2019.
- ENG participated in a workshop with the representative of Rome Municipality. ENG presented the self risk-assessment tool and collected interesting feedback. The event took place in Rome in November 2019.
- OASC participated in the inauguration of the G20 Global Smart Cities Alliance and the launch of OASC Japan in Yokohama, October 2019 where they explained there the approach of CyberSec4Europe on smart cities.
- DTU organised the DTU High Tech Summit in October 2019, where all relevant Nordic stakeholders and technology providers gathered to get to learn about advances in the area. It was a great opportunity to explain of CyberSec4Europe to potential Nordic stakeholders. GUF also attended this event.
- TU Delft participated in the New Security Paradigms Workshop (NSPW) in San Carlos, Costa Rica in September 2019. The main purpose of their participation was to collect results for questionnaires on governance requirements and data sharing.
- OASC participated in a session on critical infrastructure for smart cities organised by the Idea Factory Think Tank in Bucharest, March 2019 where they explained there the CyberSec4Europe approach on smart cities.

3.3 Scientific

Dissemination to the scientific community has been split into two different categories: publications, which include publications in journals, conferences and PhD or MSc theses; and the organisation of events, including summer schools.

3.3.1 Articles in Journals

A sample of some of these articles is listed below. The complete list can be checked on the website of the project.

- Sara Nieves Matheu, Alejandro Molina Zarca, José Luis Hernández Ramos, Jorge Bernal, Antonio Skarmeta. Enforcing behavioural profiles through Software-Defined Networks in the Industrial Internet of Things. Applied Sciences, No. 21, Vol. 9, MDPI, 2019.
- Sterlini, Pierantonia; Massacci, Fabio; Kadenko, Natalia; Fiebig, Tobias; van Eeten, Michel. Governance Challenges for European Cybersecurity Policies: Stakeholder Views. IEEE Security & Privacy, 2019.
- Luca Allodi, Marco Cremonini, Fabio Massacci, Woohyun Shim. Measuring the accuracy of software vulnerability assessments: experiments with students and professionals. Empirical Software Engineering, January 2020.

3.3.2 Articles at Conferences

Some of the articles at conferences are listed bwlow. The complete list can be seen in the ptoject website.

- Majid Salehi, Danny Hughes, Bruno Crispo. MicroGuard: Securing Bare-Metal Microcontrollers against Code-Reuse Attacks. DOI: 10.1109/DSC47296.2019.8937667. 2019 IEEE Conference on Dependable and Secure Computing (DSC). Hangzhou (China), November 2019.
- Stephan Krenn, Kai Samelin and Christoph Striecks: Practical Group-Signatures with Privacy-Friendly Openings. DOI: 10.1145/3339252.3339256. 14th International Conference on

Availability, Reliability and Security (ARES 2019), Canterbury, August 2019.

- Peter Hamm, David Harborth and Sebastian Pape. A Systematic Analysis of User Evaluations in Security Research at the 1st International Workshop on Information Security Methodology and

Replication Studies (IWSMR 2019), co-located with the 4th International Conference on Availability, Reliability and Security (ARES 2019). https://doi.org/10.1145/3339252.3340339.

- S. Ali Mirheidari, S. Arshad , K. Onarlioglu, B. Crispo, E. Kirda, W. Robertson. Cached and Confused: Web Cache Deception in the Wild. https://arxiv.org/abs/1912.10190v1. Usenix Security Conference, August 2019, Boston.
- Ulrich Haböck, Stephan Krenn. Breaking and Fixing Anonymous Credentials for the Cloud. https://link.springer.com/chapter/10.1007/978-3-030-31578-8_14. 18th International Conference on Cryptology and Network Security (CANS 2019), Springer.
- Andre Ostrak, Jaak Randmets, Ville Sokk, Sven Laur, Liina Kamm. Applying MPC for Genotype Analysis While Considering Population Stratification at Theory and Practice of Multi-Party Computation Workshop (TPMPC 2019), Tel-Aviv.
- AIT partners. Implementing a prototype for privacy-preserving analysis of money laundering data. Global Anti-Money Laundering and Financial Crime TechSprint, London, August 2019.
- Panagiotis Papadopoulos, Panagiotis Ilia, and Evangelos Markatos. Truth in Web Mining: Measuring the Profitability and the Imposed Overheads of Cryptojacking. https://doi.org/10.1007/978-3-030-30215-3_14. International Conference on Information Security, ICS 2019, LNCS, volume 11723, pp: 277-296. New York.
- Panagiotis Papadopoulos, N. Kourtelis, and Evangelos Markatos. Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask. https://doi.org/10.1145/3308558.3313542. Proceedings of the WWW '19 The World Wide Web Conference. ACM.
- Constantinos Diomedous and Elias Athanasopoulos. Practical Password Hardening Based on TLS. DIMVA 2019, pp: 441-460, Springer. https://dl.acm.org/doi/10.1145/3339252.3339256.

3.3.3 Book Chapters

- Alberto Lluch Lafuente. A Framework for Provenance-Preserving History Distribution and Incremental Reduction. Lecture Notes in Computer Science. Springer International Publishing, pp: 471-486. 2019.

3.3.4 PhD/ Master Thesis

- Letho Niko. Secured and protected management environment for blockchain keys. BSc Thesis, VTT, 2019.
- Hekkala Julius. A system that protects the use of an untrusted device in a public space. MSc Thesis, VTT, 2019.

3.3.5 Summer Schools

An important group within technical audience is that of young researchers. Therefore, the organisation and participation in summer and winter schools is a key objective for CyberSec4Europe. In this deliverable we list the schools with some involvement from CyberSec4Europe partners. The description of all the schools is provided in D9.7.

- Kai Rannenberg gave a lecture at the MISA DAAD Uni Passau IT-Security summer school, held in Antananarivo (Madagascar) in September 2019.
- IFIP Summer School on Privacy and Identity Management 2019, Brugg/Windisch, Switzerland. Several CyberSec4Europe partners were part of the organising team of the school, including:
    - Stephan Krenn, AIT (general co-chair)

  - Simone Fischer-Hübner, KAU (steering committee and programme committee)
  - Kai Rannenberg, GUF (steering committee and programme committee)
- International School on Foundations of Security Analysis and Design 2019 (FOSAD 2019). This school was held in August 2019 in Bertinoro, Italy and it was co-organised with SPARTA. As for CyberSec4Europe participants, Javier López (UMA) was a member of the scientific committee and was a lecturer too for the last edition.
- Poster Presentation at ENISA NIS 2019 Summer School by GUF. The school took place in Heraklion in August 2019 and was co-organised by FORTH.
- NeCS PhD Winter School 2020, Fai della Paganella, Italy, January 2020. This school emerged under the umbrella of the NeCS Marie Curie Training Network and it is now co-organised by the four pilots. In particular, from CyberSec4Europe Javier López (UMA) was a member of the steering committee. For the January 2020 edition, Kai Ranenberg (GUF) presented CyberSec4Europe. Also, Simone Fischer-Hübner (KAU) and Jorge Cuellar (SIEMENS) were lecturers at the school.
- KYPO Summer School on Cybersecurity organised by Masaryk University, Brno, August 2019. Partners from UM were the organisers of this school.
- The SENSYBLE Graduate School by GUF and Rhein-Main University of Applied Sciences Wiesbaden was co-organised by GUF. This school was held in Hetschbach, Germany in November and June 2019.
- GUF gave a lecture at Convite Ciclo De Palestras Internacionais UFBA, LASID/DCC/IME in Salvador da Bahia, Brazil in March 2019.

3.3.6 Organisation of Events (Conference and Workshops)

- The SRA annual meeting "Risk Analysis in the Data Analytics Era", highlighted the important role risk analysts have in tackling risk problems and improving the science and practice of risk analysis. UNITN organised a session on cyber risk as an experimental discipline with the key CyberSec4Europe topic of cyber ranges in cooperation with the US DHS, Arlington, VA, December 2019.
- 5G Security track co-located with IEEE 5G World Forum, held in Dresden in October 2019. UMA was one of the co-organisers.
- 2019 European Workshop on Security and Privacy in Edge Computing (co-located with IEEE Euro S&P), June 2019, Stockholm. UMA partners were involved in the organisation of this event.
- GUF was part of the organisation team of the ENISA Annual Privacy Forum 2019 in Rome, held in June 2019.
- DTU participated in the organisation of the 14th International Federated Conference on Distributed Computing Techniques in June 2019, which took place in Lyngby.
- DTU participated in the organisation of the Øresund Security Day in May 2019, which took place in Lyngby.
- GUF organised the PET-CON 2020.1: 11th Privacy Enhancing Techniques Convention, held in April 2019 in Germany.

3.3.7 Presentations at Events

- GUF delivered a presentation on Cybersec4Europe at the CISAR Workshop, Oslo in January 2020.
- The SRA annual meeting "Risk Analysis in the Data Analytics Era," highlighted the important role risk analysts have in tackling risk problems and improving the science and practice of risk analysis.

- UNITN presented the activities on cyber ranges, which are key activities in WP6/WP7 as well as WP3." Arlington, VA, December 2019.
- DevANDFest, organised by Google for Google Developers (GDG) in two different locations: Málaga and Granada, November and December 2019. These events are organised by Google to spread the word on their developments to developers. The talks at these events are attended by developers and also by young researchers who are interested in getting to know new technologies and work opportunities. UMA showed CyberSec4Europe, in particular, the common framework of WP3.
- Several members of GUF delivered several talks at Dagstuhl Seminar Biggest Failures in Security in November 2019.
- TDL acted as moderator on the panel ‘Cyber Security in the Healthcare Sector’ held in October 2019 at the Thon Hotel EU, Brussels, organised by JAMK and ECSO.
- TU Delft participated in the First International Scientific Conference "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE 2019) in Sofia held in October 2019. They presented the CyberSec4Europe approach to governance structure.
- GUF participated with a presentation at the TRANSFORM–Digital Skills for the Transformation of Disciplines, Business and Government event, in September 2019 in Bern.
- The 12th International Symposium on Foundations & Practice of Security, August 2019. KUL attended this conference, presenting T3.4 assets.

3.4 Business

Industry and investors are important for CyberSec4Europe as they will ultimately be the ones that will help realise the objectives and achievements of the project into real products.

- DTU participated in the organisation of the Danish Hub for Cybersecurity, which took place at the premises of DTU in Lyngby in January 2020.
- Undoubtedly, the 1st concertation meeting organised by CyberSec4Europe in Europe was the event fully dedicated to show the CyberSec4Europe objectives, goals and advances to industry and stakeholders. The event was held in Toulouse in November 2019 and all the CyberSec4Europe partners were involved in its organisation of it. Full details of this event are given in ([D10.1]).
- GUF attended the session on security research: Ensuring security and privacy in a digitising world at the European Research and Innovation Days held in September 2019 in Brussels.
- Since the start of the project CyberSec4Europe partners have had close contact with ECSO and participated in most of its events and meetings they organised. It is worthwhile highlighting the board of directors meetings attended by GUF and other partners as well as the WG6 meetings, including the one in April 2019 where CyberSec4Europe was introduced to the other members ofWG6.
- GUF participated in the Annual European Data Protection Supervisor: Internet Privacy Engineering Workshop representing CyberSec4Europe. The event took place in Rome in June 2019.
- Cyber Investors Day, Madrid, May 2019. ATOS participated in this event that brought together the most promising European cybersecurity startups to pitch their innovative solutions and participated in the strategic business matchmaking sessions. Influential European and international investors also attended the event in order to meet up with startups.

- Qualcomm organised an industry event by invitation (non-public), San Diego, May 2019. TU Delft attended this event that helped them to understand industry requirements for governance of cybersecurity to elaborate their work in WP2.
- CyberSec4Europe at the Cyber Crime Forum Wien 2019, June 2019 in Vienna. AIT participated in this event with a presentation on the ambition and goals of the project.
- GUF organised a workshop with KDDI Research. This event included a presentation on CyberSec4Europe, which was held in April 2019 in Frankfurt and another one in Tokyo in August 2019.
- OASC was invited by the Poznan Development Forum to deliver a keynote speech on the approach of smart cities by CyberSec4Europe. Poznan, October 2019.
- Cyber Investors Day in Luxembourg, October 2019. This event was a chance to meet the most innovative European cybersecurity start-ups and SMEs at the pitch sessions and the B2B meetings. Aljosa Pasic (ATOS) assisted the event and presented the project.
- Session on European Cybersecurity pilots and the impact for Spain. 13th ENISE, organised by INCIBE, October 2019 in León. This event was an opportunity to establish contacts with possible stakeholders and represent CyberSec4Europe. Aljosa Pasic (ATOS) assisted at the event and presented the project.
- Open Door CONCORDIA, Luxembourg, October 2019. This annual “Open Door Event” event, organised by CONCORDIA, was a chance for stakeholders of all backgrounds (such as legislation, industry, legal, IT) to learn more about the initiative, contribute to discussions on societal needs in the field, and to explore potential collaborations. Aljosa Pasic (ATOS) assisted at the event and gave a presentation on CyberSec4Europe.
- 21st Information Security Solutions Europe (ISSE) conference, Brussels, ATOS represented the project at this event that focused on European public and private trust related to cybersecurity, privacy, identity and Cloud and gathered together companies from Europe and beyond.

3.5 Legislative

Policymakers and administrative bodies also have to be aware of the work done in CyberSec4Europe as it will be of paramount importance to improve future legislation on cybersecurity in Europe.

- Presentation by TU Delft on CyberSec4Europe and participation in the discussion “Cooperation in EU Cybersecurity Research: Lessons (to) learn(ed)” for the bi-annual Dcypher Symposium, Utrecht, December 2019.
- TU Delft presented the governance goals and challenges of CyberSec4Europe at the EGOV-CeDEM-ePart 2019, San Benedetto del Tronto, Italy. The conference focused on e-Government, open government, eParticipation and e-Democracy, but on several other related topics too, such as the role of social media, digital transformation in society, artificial intelligence, policy information, smart governance and social innovation.
- Cybersecurity joint project workshop, held in Brussels in January 2020. Kai Rannenberg (GUF) presented the CyberSec4Europe project.
- First cybersecurity joint project workshop. 29 November 2019, Brussels. UMU, UNITN and GUF.
    - Certification tools and standardisation (UMU)
- GUF participated in the Cyber Security in the Healthcare Sector workshop held in Brussels in October 2019.

- GUF organised the meeting with Research Ministry representatives in Brussels in March 2019.
- GUF and partners organised the first public event of CyberSec4Europe on 28 February 2019 in Brussels. This evening event was attended by around 200 people including many policy makers.

3.6 Standardisation

Cybersecurity concepts need to be standardised whenever possible. For this reason, it is important for CyberSec4Europe to create liaisons with the appropriate communities. Most of the CyberSec4Europe partners are involved in standardization activities (more details are given in D8.1). We outline here a few examples of these activities.

- Periodic ISO/IEC JTC1/SC27 ("Information security, cybersecurity and privacy protection") working group meetings. CyberSec4Europe members are chairing one WG (GUF – WG5), co-editors and co-rapporteurs of multiple standardisation projects and study periods, and active contributors to multiple projects. Furthermore, CYBER and AIT requested a Category C liaison between CyberSec4Europe and WG2 and WG5. These meetings are attended by around 300 participants.
- GUF participated in the meetings of ISO/PC 317: Consumer protection: privacy by design for consumer goods and services. There were three meetings during 2019 held in February, May and October in Berlin, Toronto and Paris.
- GUF participated in the meetings of DIN KITS (German Expert Advisory Group for Cybersecurity), held in Munich in April 2019.
- GUF participated in the meetings of DIN NIA 27 AA 'IT-Sicherheitsverfahren' (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs). They were held in February and August 2019 in Bonn and Berlin respectively.
- Besides the meeting mentioned above GUF has also participated to other related meetings in the framework of DIN:
    - Meetings DIN BR-07 (German Mirror Committee to CEN/CLC JTC 13 Cybersecurity and Data Protection)
- Conference on Standardisation and Conformity Evaluation in IT Security by DIN, German Federal Ministry for Economics and Chinese partners. Berlin, February 2019.

4 KPI Achievements

[D9.3] also identified the list of KPIs that will indicate the success of CyberSec4Europe in relation to the activities listed above as shown in Table 2. We will describe here how CyberSec4Europe partners have performed in relation to these KPIs. Note that the timeline target of these KPIs is for the whole period of the project, therefore, they could not be completely achieved but some of them are to be achieved annually and, they could be measured by M12. For the others, if some results are in place, it is a good indicator that the communication strategy is heading in the right direction.

Activity	KPI/Target	Achieved
Flash studies, production of CyberSec4Europe leaflets	≥ 3, one per annum	9
Participations in 6 public exhibitions and demonstrations	3 per annum after M12	Already carried out, however it was expected after M12
Journal publications in international referred journals	More than 30	5
Reviewed publications/presentations in international conferences	More than 50	17
CyberSec4Europe co-organised workshops	More than 2 workshops, each attended by more than 40 participants, with more than 20 external	7
CyberSec4Europe tutorials	More than 2 tutorials co-located with summer-schools, more than 1 in a relevant conference	
Organization and hosting of 4 hackathons/ pitstops	To take place after M12	
6 presentations at meetups	2 per annum after M1	20
CyberSec4Europe newsletters through social media dissemination and news on website	6 newsletters with 1 issue/participation	5

Table 1 First year KPI results

- **Flash studies, production of CyberSec4Europe leaflets.** As part of the dissemination material we designed different printed material. They are described in ([D9.2], 2019). We designed a brochure, a general poster and a poster for each of the CyberSec4Europe demonstrator use cases. Therefore, we have delivered for the first year nine of these flash studies, which is more than the one expected per year.
- **Participations in six public exhibitions and demonstrations.** Several partners have already carried out this activity, however it was expected to take place after M12.
- **Journal publications in international referred journals.** The partners of CyberSec4Europe are very well-known researchers and therefore they are very productive in terms of publications in both international conferences and articles in referenced journals. At the moment, CyberSec4Europe partners have published five journal papers but there are many papers submitted for review that hopefully will be published during the second year of the project.

- **Reviewed publications/presentations in international conferences.** In terms of publications in international conferences the CyberSec4Europe partners have published seventeen international conference papers, which were presented in the corresponding venues.
- **CyberSec4Europe co-organised workshops.** During the first 12 months of the project, CyberSec4Europe partners have been involved in the organisation of three workshops. They have organised these events in cooperation with other communities and researchers. The workshops organized by some partners were the following:
  - 2019 European Workshop on Security and Privacy in Edge Computing (co-located with IEEE Euro S&P). Stockholm, June 2019.
  - 5G Security track co-located with IEEE 5G World Forum. Dresden, October 2019.
  - 1st Cyber Security joint project workshop. Brussels, November 2019.
- **CyberSec4Europe tutorials.** During the first 12 months, CyberSec4Europe partners had not yet organised any tutorials in summer schools. However, we are expecting to organise several of these tutorials during the next coming year.
- **Organisation and hosting of four hackathons/ pitstops.** As indicated in Table 2 these activities will only be considered after M12.
- **Six presentations at meetups.** At M12 CyberSec4Europe partners have attended already more than six meetings and have presented their work at more than six events, therefore by the end of the project this figure will increase.
- **CyberSec4Europe newsletters through social media dissemination and news on website.** The website is the main channel for publishing project news. At the time of writing, six news items have been published there. Five of them are related to the concertation event that took place in Toulouse in November 2019. The other one announces the deliverables available on the website.

  The website News page on the website includes several blog posts that describe project work that or some relevant advances. As mentioned in ([D9.3]), CyberSec4Europe partners were expected to produce clear and accessible articles, capable of being understood by non- specialist high-level audiences such as policy makers, senior enterprise managers and civic leaders. The first of these blog posts was published on 28 November 2019, since then, the blog posts have included articles on different topics of the project:

  - Common Framework for CyberSec4Europe.
  - Assessing Cybersecurity Risks using “capture the flag”.
  - Identifying Cross-Sector Enablers for Privacy and Cybersecurity.
  - Research Challenges and Requirements to Manage Digital Evidence
  - Designing a Governance Structure for Europe’s Cybersecurity Community.

5 Joint Activities with the other Three Pilots

The four pilots funded under the call SU-ICT-03-2018 call (CONCORDIA, ECHO, SPARTA, CyberSec4Europe) share a common purpose which is to establish and operate a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap. Thus, since they all started, DG CNECT has worked closely with them to show that, even though their work on their topics on cybersecurity topics varies, they share the common goal of piloting a future Cybersecurity Competence Centre.

The four pilots' communications group was set up specifically to coordinate common dissemination and communication activities and to give a unique look to the work the four pilots do together. One of the main outcomes was the creation of a common website for the four pilots[1]. Each project is responsible for contributing to the website and other activities on a rotating six-monthly basis.

The activities that CyberSec4Europe has participated in as part of the four pilots' communication group are listed below.

- TDL was responsible for designing a logotype and branding for the activities of the four pilots, including the design for the common website (hosted by ECHO), as discussed in the communications group. The website was formally launched on stage by Despina Spadou and others at the evening social event of the CONCORDIA General Assembly with a 'red button' symbolically being pushed. June 2019.
- Periodic conference calls took place with representatives of the four pilots and Konstantinos Ntantinos in formulating plans for the Communications Group, particularly the creation of a common brand and website. February - May 2019.
- David Goodman and Christine Jamieson (TDL) attended an all-day meeting at the invitation of CONCORDIA, together with representatives from ECHO and SPARTA as well as three representatives from DG CNECT, including Konstantinos Ntantinos at the Representation of the Free State of Bavaria to the European Union, Brussels, March 2019.
- Working in collaboration with DG CNECT and the other three pilot representatives, TDL published a press release concerning the commencement of CyberSec4Europe that was broadcast simultaneously with similar announcements made by DG CNECT and the other three pilots.

Besides these activities in the framework of the communications group, a CyberSec4Europe representative participated in numerous events involving the four pilots.

- cyberwiser.eu Open Pilots Workshop organized by the Cyberwiser project and held in Domus Comeliana, Pisa in November 2019. David Goodman (TDL) represented CyberSec4Europe together with representatives from the other three pilots, namely Matteo Merialdo (ECHO), Fabio Martinelli (SPARTA) and Claudio Ardagna (CONCORDIA) at the panel 'EU Cybersecurity Network & Competence Centres: How your organisations will benefit?'

[1] https://cybercompetencenetwork.eu/about/

An important outcome of this event was that Nick Ferguson was invited to participate in ‘Cybersecurity For Europe 2019’ in Toulouse. CyberSec4Europe represented by T9.4 will share a stand with Cyberwiser at the FICO Conference on 28-29 January 2020.

- At the 27th Meeting of the Horizon 2020 Programme Committee configuration for Secure Societies held in Brussels in October 2019, David Goodman (TDL) represented CyberSec4Europe together with representatives from the other three pilots, namely Gabi Dreo (CONCORDIA), Florent Kirchner (SPARTA) and Wim Mees (ECHO). The meeting was chaired by Turo Mattila. The four pilots’ session was introduced by Miguel Gonzalez-Sancho-Bodero (DG CNECT), with CONCORDIA providing the four-pilot overview. The title of the panel was ‘Collaborative activities within the cluster of the four EU pilots on Cybersecurity competence network’.

- CONCORDIA organised the CODE 2019 conference at the German Military University, Munich in July 2019. David Goodman (TDL) represented CyberSec4Europe together with representatives from the other three pilots, namely Thibaud Antignac (SPARTA), Matteo Merialdo (ECHO) and AN Other (CONCORDIA). The moderator was Rafael Tesoro-Carretero (DG CNECT). After our individual presentations, Rafael posed the following questions:
    1. Each pilot was asked to look at the other three projects and to tell about one good thing from (one/all three) of the peer pilots that might be somehow missing in or complement their own pilot.
    2. The four pilots were asked to work together maximising synergies and minimising overlaps.
        a. What are the main challenges for 160+ partners working together?
        b. How do we plan to appeal and attract to the network others beyond the four pilot consortia?
        c. How do we envision the dynamics of the forthcoming Cybersecurity Competence Network, which is starting to be shaped by the four pilots?
    3. What are the pilots’ views about key technological and industrial priorities of cybersecurity in the EU? Can we name a few of these priorities?
    4. In which concrete ways will the pilots contribute to the European strategic autonomy in the field of cybersecurity?

- The CANVAS project organised a workshop at the Vrije Universiteit Brussels in June 2019. David Goodman (TDL) represented CyberSec4Europe together with representatives from the other three pilots, namely Thibaud Antignac (SPARTA), Wim Mees (ECHO) and Vassilis Prevelakis (CONCORDIA). Being aware of the synergies that might appear between CANVAS and CyberSEc4Europe, a representative of CANVAS gave a presentation session at the CyberSec4Europe General Assembly on 4 July 2019.

- The COMPACT project organised a workshop (in tandem with the Major Cities of Europe conference) at Ca’ Foscari, Venice. David Goodman (TDL) represented CyberSec4Europe together with two other CyberSec4Europe partners, Davor Meersman (OASC) and Fabio Massacci (UNITN) on the panel ‘Cybersecurity solutions for Local Public Administration’. A representative of COMPACT (Marco Angelini, ENG) gave a presentation to the WP9 session during the

CyberSec4Europe General Assembly on 4 July 2019, which may lead to further collaboration in the context of T9.4.

- The ID2020/SEREN4 projects including the national contact points for cybersecurity organised the Unit H1 Concertation Meeting in Luxembourg in June 2019. David Goodman (TDL) represented CyberSec4Europe at the panel 'Meet & Talk workshop'. Together with TDL, members of the other pilots participated to the panel. In particular, Matteo Merialdo (ECHO), Géraud Canet (SPARTA) and Olivier Festor (CONCORDIA). The pilots were asked to make a presentation different from the one we were usually doing in front of "usual" dissemination audiences and were asked to focus on the following points:
  - What are the industrial verticals your pilot is covering?
  - What is your pilot's view on what will be the outcome of the 4 pilots (a foundation, the EU research centre, a merging… what are your view on that)?
  - How do you see the future of your pilot in the next 2 years and what related NCP activities can we help you with?

  Following the workshop, the pilot representatives were asked to participate in World Café sessions with the national contact points and discuss the following:

  - Cooperation and synergy of the four projects – what has been done and what is planned for the future - How can we link better the NCP and the pilots?
  - What new services to proposers/participants can the NCP/NCP projects offer with the support of the pilots (and vice-versa)?
  - What future NCP services or national support can be foreseen at the end of the pilots?
  - International collaboration: what are the planned actions in relation with Associated Countries and what international activities are foreseen, especially in terms of standards?

- The Cyberwatching.eu project organised a Unit H1 Concertation Meeting at the Marriott Grand Palace Hotel, Brussels in June 2019. CyberSec4 Europe was invited to participate in the panel 'Building a cybersecurity ecosystem to secure European society'. David Goodman (TDL) represented CyberSec4Europe on the panel with representatives from the other three pilots, namely Gabi Dreo (CONCORDIA), Géraud Canet (SPARTA) and Wim Mees (ECHO). The session was moderated by Nick Ferguson. Each of the pilots were asked to discuss their own approaches to the following topics:
  - Cyber ranges
  - Threat intelligence
  - Certification
  - Cybersecurity skills
  - Collaboration between the projects

  Each of the panelists took part in ten-minute interviews after the session and were asked to respond to the following four prepared questions:

  1. In order to pilot the Cybersecurity Competence Network: How will the operational & substantive cooperation be achieved among the 4 pilots and beyond?
  2. How does your pilot interconnect with Europe's Cybersecurity capabilities?

3. Do you think it's possible to achieve Digital Sovereignty of Europe? What are the main challenges?
4. How do you imagine the Cybersecurity landscape in Europe in 5 years from now on?

The interviews were filmed and the material was collated and edited together to eventually be posted as a streaming video on the homepage of the common website [2].

- DG HOME in collaboration with DG CNECT organised a Community of Users event held in the BAO Congress Centre, Brussels in March 2019. David Goodman (TDL) acted as speaker coordinator for and attended the panel ‘Building a cybersecurity ecosystem to secure European society’. The moderator was Sebastiano Tofaletti, Secretary General European Digital SME Alliance and partner in Cyberwatching.eu. The speakers were Rafael Tesoro Carretero (DG CNECT), Lea Hemetsberger (CyberSec4Europe), Géraud Canet (SPARTA), Felicia Cutas (for Gabi Dreo) (CONCORDIA) and Douglas Wiemer (ECHO).
  A well-edited video based on the four interviews was produced and published on the four pilots’ website.
- GUF attended the launch event of the ECHO project in February 2019 in Brussels (Belgium).

DG CNECT Unit H1 has organised meetings periodically with the four pilot project coordinators. Kai Rannenberg has attended all of them. These meetings have to date generally been organised on a monthly basis. Thus, since the beginning of the project Kai Rannenberg represented CyberSec4Europe in nine meetings. Some of these meetings have also been attended by representatives of REA or JRC. For the meeting held in March 2019, the four pilot coordinators also had a meeting with Commissioner Gabriel at the European Parliament in Strasbourg. Also, in November 2019 the four coordinators held a meeting with MEPs on Cybersecurity Competence Network at the European Parliament in Brussels.

[2] https://cybercompetencenetwork.eu/about/

6 Conclusion

In this deliverable we have described the outreach activities carried out by CyberSec4Europe partners during the first year report of the project. We have described these activities by following the target audiences identified in ([D9.3]).

We have referenced the KPIs that will determine the success of the project. These KPIs are related to the organisation of meetings, workshops, publications, the use of dissemination material or participation in summer schools. The analysis of these KPIs indicate that, after the first year of the project, the outreach activities are well in advance of the expected outcomes at this stage of the project.

A very important part of the dissemination activities comes under the umbrella of the four pilots' communications group, organised with the other three pilots. CyberSec4Europe plays a key role in this group.

7 References

[D10.1]. (s.f.). *Clustering results and SU-ICT-03 project CONCERTATION Conference Year 1. January 2020.*

[D10.1]. (s.f.). *Clustering results and SU-ICT-03 project CONCERTATION Conference Year 1. January 2020.*

[D9.2]. (2019). *Dissemination material: Brochures, poster. May 2019.*

[D9.3]. (s.f.). *Dissemination and Awareness Plan. Cybersecurity for Europe deliverable. August 2019.*

[D9.4]. (s.f.). *Website and Social media accounts 2.*

[D8.1]. (s.f.). Cybersecurity Standardization Engagement Plan