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

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D9.3
Dissemination and Awareness Plan

Document Identification	
Due date	31 July 2019
Submission date	9 August 2019
Version	1.0

Related WP	WP9	Dissemination Level	Public
Lead Participant	TDL	Lead Author	Christine Jamieson (TDL)
Contributing Beneficiaries	DTU, NTNU, UMA	Related Deliverables	

Abstract: This document describes the dissemination and awareness planning in support of the objectives of the CyberSec4Europe project, in terms of both internal and external communications and dissemination initiatives as was well as an indication of the possible future direction and plans of the coordinated Communications Group of the four pilots.

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.

Executive Summary

This document provides details of CyberSec4Europe project's communication and dissemination strategy as well as development plans for future stages of this strategy as the project progresses.

This report defines both the narrative for CyberSec4Europe and the target audiences for the project. It details the most appropriate channels to reach these groups and examines various methodologies to best achieve awareness.

The document also includes details of the project's joint strategy for aligning its message with that of the other three pilots. It also explains how this cooperation between the pilots will strengthen the overall message to the various audiences throughout the EU.

The CyberSec4Europe communications strategy will evolve significantly during the course of the 42 months – it aims to be flexible and agile as project results are achieved and the project's end point takes shape. It will also be responsive to external events in the sphere of cybersecurity. How these changes, and their impact with relevant stakeholders, develop will be the subject of continuous evaluation reports [D9.5, D9.9, D9.10, D9.13, D9.18, D9.23 and D9.26].

Document information

Contributors

Name	Partner
Christine Jamieson	TDL
David Goodman	TDL

Reviewers

Name	Partner
Jozef Vyskoc	VaF
Marco Angelini	ENG

History

0.1	4 August 2019	Christine Jamieson	Initial draft

List of Contents

List of Figures

List of Tables

List of Acronyms

ACM	Association for Compuing Machinery
COMPACT	Cybersecurity for Public Administrations
CONCORDIA	Cybersecurity Competence for Research and Innovation
DTU	Technical University of Denmark
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
ECSO	European Cyber Security Organisation
ENG	Engineering Ingegneria Informatica Spa
ENISA	European Union Agency for Network and Information Security
IEEE	Institute of Electrical and Electronics Engineers
IERC	The International Energy Research Centre
IFIP	International Federation for Information Processing
IOT	Internet of Things
JAMK	Jyväskylän ammattikorkeakoulu (University of Applied Sciences)
LPA	Local Public Administration
NTNU	Norwegian University of Science and Technology.
SDO	Standards Developing Organisation
SME	Small to Medium-sized Enterprises
SPARTA	Strategic Programs for Advanced Research and Technology in Europe
SU-ICT	Security Union
TDL	Trust in Digital Life Association
UMA	University of Malaga
WP	Work Package
WP6	Cybersecurity Skills & Capability Building
WP9	Dissemination, Outreach, Spreading of Competence, Raising Awareness
WP10	Community Empowerment & Innovation Fostering

1 Introduction

1.1 CyberSec4Europe – defining the narrative

CyberSec4Europe is – simply put – about demonstrating ways that European industry and academia can work together to boost the security of all citizens and organisations in their everyday digital transactions.

To that end, the project aims through a number of ways, across a variety of private and public sectors, to establish best practice for ensuring maximum security and effective information sharing.

The context for CyberSec4Europe is however part of a wider story. The creation of a Digital Single Market has been a principal goal of the EU for many years. One of the project's key goals in helping to achieve this ambition is to design a way in which a perfectly coordinated network of experts in the field of digital security can work together as effectively as possible to ensure that any potential disruptors to that market, whether through malicious attack or systems failures, are anticipated and eliminated.

This straightforward narrative conveys why the project exists and why it matters.

A more expanded version of this narrative comes from the call for proposal **SU-ICT-03-2018 - Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap**[1]**:**

> *"EU's strategic interest is to ensure that the EU retains and develops essential capacities to secure its digital economy, infrastructures, society, and democracy. Europe's cybersecurity research, competences and investments are spread across Europe with too little alignment. There is an urgent need to step up investment in technological advancements that could make the EU's digital Single Market more cybersecure and to overcome the fragmentation of EU research capacities. Europe has to master the relevant cybersecurity technologies from secure components to trustworthy interconnected IoT ecosystems and to self-healing software. European industries need to be supported and equipped with latest technologies and skills to develop innovative security products and services and protect their vital assets against cyberattacks. This should contribute inter alia to achieve the objective of European strategic autonomy."*

This statement highlights several important background issues – the urgency of the task, the lack of connectedness in current research, the need in the current geo-political climate for digital sovereignty.

[1] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018;freeTextSearchKeyword=;typeCodes=1;statusCodes=31094501,31094502,31094503;programCode=H2020;programDivisionCode=null;focusAreaCode=null;crossCuttingPriorityCode=null;callCode=H2020-SU-ICT-2018-2020;sortQuery=openingDate;orderBy=asc;onlyTenders=false;topicListKey=topicSearchTablePageState

CyberSec4Europe's main objective within that narrative framework is to pilot the consolidation and projection into the future of European-wide cybersecurity capabilities required to secure and maintain a European democracy and a world-leading digital economy.

In practical terms, this means the creation of a new digital ecosystem, or network of centres of cybersecurity expertise, with a centralised coordination point – a Cybersecurity Competence Network hub. It also means the creation of a Europe-wide roadmap for research and innovation. This will be enacted as legislation in 2020.

Dissemination and awareness of the pilot's progress are key to meeting that objective. H2020 programmes are about securing Europe's global competitiveness, and the CyberSec4Europe consortium partners have a responsibility to 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.

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 the results.

1.2 What the dissemination and awareness plan will achieve

The plan, when implemented, will:

- assist CyberSec4Europe achieve its overall project objectives. It will be a reference document against which to judge CyberSec4Europe's progress;
- ensure that CyberSec4Europe engages effectively with its multiple stakeholders;
- identify the relevant channels for the message;
- promote the success of the project's work;
- ensure people understand what CyberSec4Europe does;
- change behaviour and perceptions of businesses/organisations/citizens to the threats of cyber attacks and the precautions to be taken against them.

In order to complete these goals, it is vital that this plan:

- has **clear and measurable communications objectives** with the necessary evaluations to judge their success;

- has a **set of activities** and a **timetable** for achieving those activities;
- has several staged **review periods** to ensure that it is still fit for purpose as the project advances.

The plan is a collaborative effort, that must be jointly owned by all members of the project;

2 Target Audiences

The potential audiences for CyberSec4Europe are extremely varied and diverse, each with its own characteristics and associated perspectives and messages pertaining to cybersecurity.

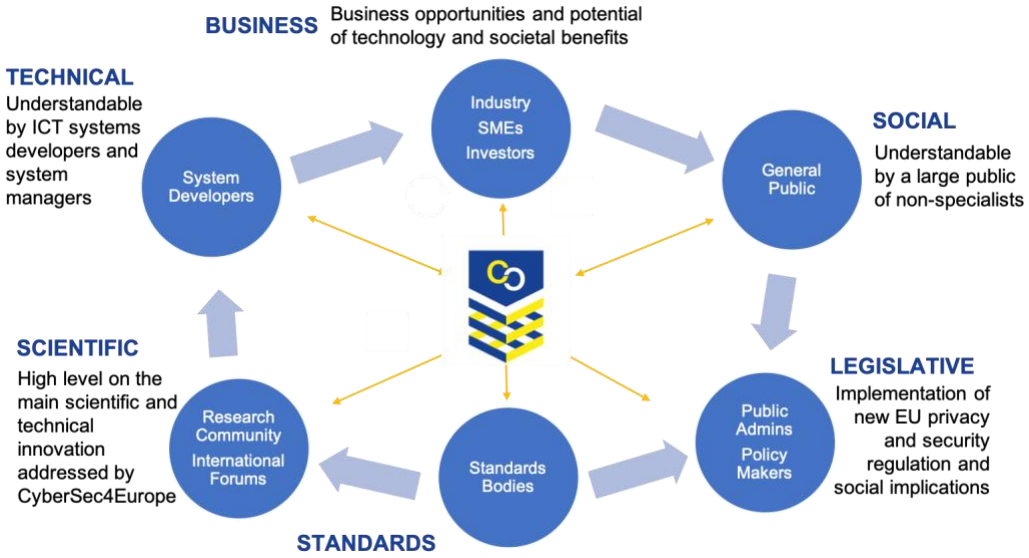

Figure 1: Cybersecurity stakeholders

2.1 Defining the target 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 CS4E	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; Societal benefits 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: Stakeholders, messages and channels

3 Communication and Dissemination

The Commission differentiates between communication and dissemination as two separate but inter-related activities. The defining characteristic of each activity is the intended audience.

- **Dissemination** is the spreading of results and best practice both on a peer-to-peer basis and across to industrial stakeholders and policy makers.
- **Communication** is aimed at a wider audience with a number of sub-sets. At a fundamental level, it can mean every European citizen.

Figure 2: Communication and dissemination objectives

Figure 3: Communication and dissemination channels

On a practical level, it will be a strategic mixture of the audiences that can most effectively be targeted with existing channels, and ones who might be reached through a number of innovative approaches. CyberSec4Europe plans to undertake both types of activity, and its wide partner base allows it the ideal opportunity to do so.

4 Key Objectives

The key high level goal of WP9 is to inform about the cybersecurity pilot project and promote its role in supporting EU's existing and future cybersecurity policy initiatives especially the Cybersecurity Act and the cybersecurity competence centre and network legislation. Although CyberSec4Europe is 'only' a pilot with reasonably limited resources and cannot do everything that needs to be done, nonetheless the key is to demonstrate what has to be done with excellence.

The messages will vary according to the type of audience but the overall intention is:

- to promote the work of the EU in this domain to the **general public:** as well as to explain why EU invests this amount of money in these pilots and more generally in cybersecurity;
- to develop the European **cybersecurity ecosystem** as well as to enhance contact with the pilot projects and their deliverables.

Each aspect of the project – each task and each workpackage – has a great story to tell, and we have a shared responsibility across the project to build the stories and communicate them.

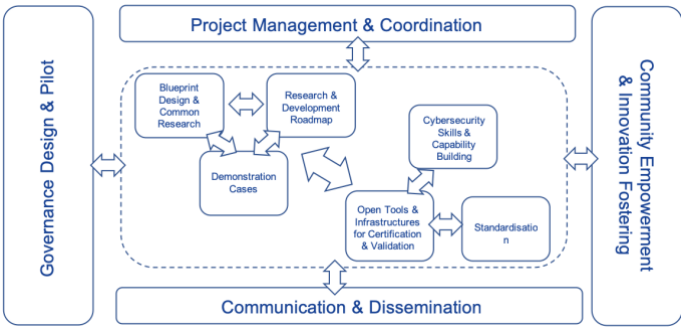

Figure 4: Interconnected workpackage clusters

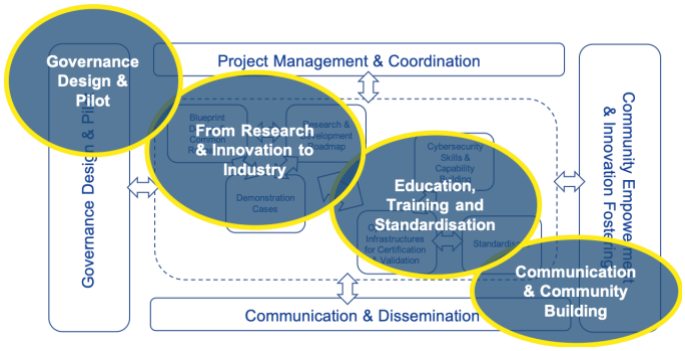

Figure 5: Workpackage cluster narratives

5 Communications

The specific non-technical audiences that CyberSec4Europe will reach out to is broad, each with its own important rationale. The project will raise cybersecurity awareness across industry and society by establishing the value of new integrated secure and trust-aware services involving where possible end-users in piloted activities. One essential target group is SMEs, a sector that constitutes the overwhelming majority of enterprises (approximately 99%) in the EU and which accounts for two out of every three jobs (Eurostat 2016). Many SMEs are sub-contractors to large enterprises operating in industrial sectors, critical for the security maintenance of national supply infrastructures. One focus will be on the potentially serious cybersecurity problems that these SMEs may generate for a whole supply chain.

The rationale for raising cybersecurity awareness of the general public is no less critical. Whilst the process of digitisation has brought unprecedented growth in the EU, the rise of cybercrime has also diminished citizens' confidence. The rapid development of poorly secured IoT devices and the spread of 5G, with the huge amounts of data they generate, will make this challenge even more urgent as the general public's level of security awareness is not at the level necessary to tackle the potential threat of cybercrime. Human error, in other words actions that were unintended or accidental, is the leading cause of data and security breaches. The most common types of breaches occur as a result of someone sending data to the wrong person. Educating citizens about the potential consequences of their actions is one of the main challenges that needs to be met by a well-considered and creative communication strategy. No less important is the notion of creating or re-establishing trust in cyberspace, which suggests not only the minimization of human errors, but also improved resistance to falsification, phishing, frauds, and other forms of attack.

5.1 Communications roles within the project

WP9 is responsible for managing the communications activity within the lifetime of the project (and beyond) – not simply as a one-time formality at the end of the project. In practice this means, *inter alia*:

- creating content and updating the website and social media accounts;
- drafting press releases;
- coordinating position papers and/or consortium statements reacting and reflecting on important events such as security incidents produced by consortium members;
- acting as a liaison point for press and other media;
- commissioning any graphic design work and managing the correct implementation and usage of the CyberSec4Europe brand;
- liaising, if appropriate, with other workpackages in their dissemination activities;
- liaising with the EC on communications matters where necessary and using EC channels where available.

However, the duty to communicate falls on all members of the project – there is a contractual obligation to ensure that all partners can effectively explain their work to the European taxpayer, demonstrate the added value and positive impact of the project. Additionally, it is up to individual WP and task leaders to help the communications team identify specifically who would be their target audience, who would be interested in their results and who will be directly affected by the outcome of their research. For example, this could be the banking sector for the relevant demonstration use cases[2]. The WP9 team will act as a central resource to assist and advise colleagues with this task. The team will also help ensure there is a consistency of message and tone when communicating results.

6 Communication and raising awareness with European citizens

The challenges for CyberSec4Europe to reach the general public are:

- similar to those facing any large scale EU-wide pilot that attempts to convey its message to a very large non-specialist audience in a meaningful and engaging way;
- the perennial challenge of finding the correct method/channel to reach a very large heterogeneous audience, not only to impart valuable information but also to use that message to "nudge" people's behaviour pattern towards a more desirable outcome – in this case, to act positively upon a greater awareness of the risks they face when digitally transacting.

[2] Task 5.1 Open Banking and Task 5.2 Incident Reporting

6.1 The wider citizen audience and its components.

The general public is an unhelpful term when trying to describe the multiple audiences that CyberSec4Europe is tasked with trying to reach. At its most fundamental, it is a collection of over 500 million people of hugely varying backgrounds, demographics and cultures. Yet every citizen on-line in Europe has a role to play in maintaining a healthy and secure cyber eco-system. The strength of the consortium is its vast spread of participating countries and organisations. Using the experience of the 43 partners, it makes sense to target specific groups within the wider community to pilot a number of communications exercises. These pilot studies can be used to monitor and evaluate what methodologies are most successful in both raising awareness and changing behaviours.

6.2 The role of SMEs

The pivotal role of SMEs in the European Digital Single Market has already been outlined in this report, and it is one of the priorities of CyberSec4Europe to study different approaches to reaching this huge and disparate category through a number of carefully coordinated pilots, each focussed on a particular sector.

The sectors that have been chosen for pilot studies are:

- Health
- Local Public Administrations (LPAs)
- Education

Each of these sectors represents a huge variety of sub-groups – employers, sub-contractors, consumers, citizens, students. Studies and results on usability and security awareness can complement CyberSec4Europe's established knowledge and processes across secure systems engineering, significantly enhancing the security posture of organizations but also society at large.

By using the contacts networks of the partners within the consortium, these sub-categories will be further refined to form manageable focus groups and chosen to participate in a number of studies.

CyberSec4Europe will be looking within its established networks for the following types of organisations that:

- can contribute with targeted data collection at a national or regional level;
- would be interested in getting involved with the development of methods for data collection, analysis, continuous monitoring etc;
- would be interested in getting involved with the dissemination of results (i.e. mechanisms, recommendations, statistics).

It will be critical to provide increased visibility of the results of each exercise, in turn adjusting both the message and the medium to the requirements, objectives and viewpoints of the corresponding stakeholders.

Supporting press and social media campaigns will be developed with partners to identify potential focus groups, requesting volunteers come forward for the pilot studies.

6.3 Methodologies and pilot study categories

The participants in WP9 will coordinate the different focus groups within their chosen specialist sector. For example:

- UMA will run a series of focus groups reaching out to young people through its university entrance procedures when large groups of school children visit the UMA campus as an information-gathering exercise before applying.
- JAMK will focus on reaching out to their links with health providers, a large group that may have several sub-categories such as doctors and medical staff through to patients.
- Potential LPAs will be sought through links with colleagues in the smart cities task (WP5.7 Smart Cities) and also build on work undertaken by other partners in raising cybersecurity awareness such as the work of the COMPACT project undertaken by ENG.
- The latter will be informed by studies carried out by NTNU on cybersecurity awareness in rural communities, or on digital natives. NTNU has extensive experience of survey modelling, running focus groups, analysis of data outputs and re-testing.

Although these examples are necessarily of a local/national nature, the intention is that these pilot studies are potentially scalable to a wider international audience and will demonstrate best practice.

6.4 Innovative methods for reaching citizens and changing behaviours

As a result of the data collected through these focus groups, Task 9.4 (Raising Awareness) will examine new ways to reach target audiences beyond the traditional means of dissemination. For example given that digital natives are unlikely to engage with printed information leaflets, however well-designed, but are more likely to view on-line content, the group will look at what specific channels would be more successful, and how the messages carried through those channels should be refined to actually encourage behaviour modification towards desired outcomes.

6.5 Linkage to WP6 (Cybersecurity Skills and Capability Building)

As WP6 is responsible for setting an education and training framework for citizens, students and professionals, there is scope for crossover collaboration between WP6 and WP9. The work of WP9 can certainly be informed by the preliminary research undertaken in Task 6.1 (University Education) as they set about mapping the national requirements of Members States and Associated Countries to identify the cybersecurity skills framework to be used as a reference by education providers.

7 Dissemination

CyberSec4Europe aims to maximise dissemination of the project results to a wide audience of researchers and technologists within the relevant cybersecurity communities and initiatives. These dissemination activities are seen as a necessary step before and during the exploitation of the project results. It should also be noted that another essential target audience for this dissemination work are media, including specialist ICT and industry media to reach even greater audiences.

7.1 Dissemination in practice

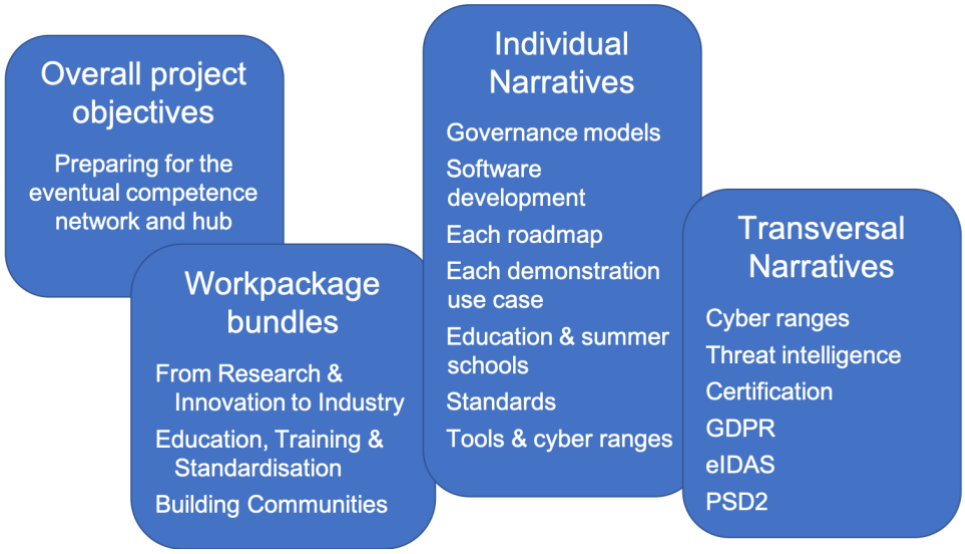

Figure 6: CyberSec4Europe's dissemination activity

Dissemination of CyberSec4Europe's progress and activities is in practice a more straightforward activity with a relatively stable set of existing channels and framed in the same technical language that most researchers will be working within. The overall project objective will be clear and familiar to the intended audience of stakeholders from the outset, and the significance of the individual and transversal narratives will be easily grasped. This is not to say that this activity needs little effort or is simply being undertaken to fulfil the commitments of the Grant Agreement! It should be thorough, systematic and continuous. This peer-to-peer dissemination should in fact be a dialogue between project partners and a number of key stakeholders such as the scientific community, industry, policy makers and legislators, and standards bodies (SDOs).

7.2 Peer-to-peer dissemination

Peer-to-peer dissemination should happen in any research project for the following reasons:

- it helps spread excellence and guidance on best practices in next generation industrial and civilian cybersecurity technologies, applications and services;

- it creates and maintains a dialogue between fellow researchers;
- it enables research communities in the same field to cluster and create collaborative partnerships;
- it stops researchers working in isolation, and avoids duplication of effort.

7.2.1 Peer-to-peer dissemination activities

The dissemination activity will focus on the collection and promotion of:

- publications in high-quality scientific journals, such as ACM and IEEE Transactions;
- presentations in specific influential, high-impact conferences related to cybersecurity such as ACM Conference on Computer and Communications Security, IEEE Security and Privacy and USENIX Security;
- organisation of workshops such as the International Symposium on Engineering Secure Software and Systems (ESSoS), conferences, special sessions, tracks, etc.;
- participation and contributions in other relevant conferences and workshops including those organized by the European Commission, IERC, IFIP and other relevant organisations such as the IoT Forum, IoT Week and IoT TechExpo;
- dissemination through several summer schools;
- collocating workshops with conferences that several participants co-chair regularly.

7.2.2 The tools for peer-to-peer dissemination

- **Publications and presentations databases**
  WP9 partners have created two proformas for all partners to report their publication activities and events participation activities. Partners will be issued with periodic reminders to keep these up-to-date throughout the lifecycle of the project.
- **Project website**
  The CyberSec4Europe website will host this large repository of publications, articles and keynotes collated from the above database. This will be continuously updated and monitored. Similarly, the website will also have a comprehensive listing of all events that CyberSec4Europe project members are involved in, highlighting what specific contribution the project partner will make to the proceedings e.g. keynote address, presentation of a paper.
- **Flyers/templates/publicity material**
  WP9 partners can assist colleagues in producing the necessary artwork for project representatives who are attending events in the name of CyberSec4Europe, employing the correct usage/styling of the CyberSec4Europe branding.

To date WP9 has made available:

- Long and short Powerpoint presentations
- A4 generic posters

- Nine extra large posters (for the Kick Off launch event)
- A4 information flyer
- Press release (for the project launch)
- Four pilots' (Cybersecurity Competence Network) infographics

The next phase of publicity material will include, *inter alia*:

- A series of short- to medium- Powerpoint presentations, broken down by Work Packages, tasks, transversal themes
- An internal communication guide – how we best communicate news and stories amongst each other and externally
- A template for roll-ups
- Press releases – based on project events and the main deliverable cycles

7.3 Industrial Dissemination

Industry will be targeted by the participation of CyberSec4Europe members at relevant events to promote and demonstrate the results and the potential.

The project will organise presentations and workshops for companies to describe the main features and benefits of the project to obtain feedback as well as an environment that encourages and actively supports buy-in of the project results. Many of the project participants are regularly invited to present at events targeted at government, authorities and company decision-makers. This will allow CyberSec4Europe to present the project results at these venues as well.

Whitepapers which showcase CyberSec4Europe industrial use cases and benefits will be presented to communities such as:

- **ECSO**: The cybersecurity is for industry and academia to define the Strategic Research Agenda where, for example, GUF and UMU are active and contribute in different WGs. CyberSec4Europe could bring different aspects of solutions to several WGs, for example, related to the certification of security services and systems.
- **Trust in Digital Life (TDL)**: TDL is a not for profit membership association that counts several CyberSec4Europe partners as members. Of relevance to the project, it addresses aspects of user-oriented security and privacy as well as artificial intelligence and open banking. CyberSec4Europe can contribute to the identification of privacy aspects related to the impact of the GDPR on privacy tools.

This activity is closely linked with the work of WP10 (Community Empowerment & Innovation Fostering) that is focussed on community building, primarily through three major annual concertation events, the first one of which will take place in Toulouse from 13-15 November 2019.

7.4 KPIs/Targets

Activity	KPI/Target
Flash studies, production of CyberSec4Europe leaflets	≥ 3, one per annum
Participations in 6 public exhibitions and demonstrations	3 per annum after M12
Journal publications in international referred journals	≥ 30
Reviewed publications/presentations in international conferences	≥ 50
CyberSec4Europe co-organised workshops	≥ 2 workshops, each attended by ≥ 40 participants, with ≥ 20 external to project
CyberSec4Europe tutorials	≥ 2 tutorials co-located with summer-schools, ≥ 1 in a relevant conference
Organization and hosting of 4 hackathons/ pitstops	≥ 2 per annum after M12
6 presentations at meetups	2 per annum after M1
CyberSec4Europe newsletters through social media dissemination and news on website	6 newsletters with 1 issue/participation every 6 months

Table 2: Key performance indicators

7.5 A timetable for the communications and dissemination tasks

By M12, when the various outputs from each workpackage start to become available, WP9 will produce a set of annual timetables for both communications and dissemination activities. Each one will show what specific activities will be planned for each month and these will be internally circulated at the beginning of each year so that participants understand at what point the various news cycles are, and how they should factor this into their communication of results. It will also be the responsibility of WP9 to assist colleagues with any ad hoc communications activities, such as responding to unplanned, external events.

8 Internal Communication

A consortium of 43 partners clearly needs effective internal communications channels. In addition to the formal management reporting processes, WP9 is proposing a number of creative ways in which internal news and results can be also be disseminated among partners.

One important task of WP9 is to help facilitate clear communication between the partners themselves, to help support them in keeping a bird's-eye view of the progress of the project, and ensure that each WP leader is aware of any related activity in other WPs that may have some linkage to their own work.

The benefits are transparent – the project represents an enormous opportunity for forging links between researchers in different institutions, creating new partnerships and collaborating to achieve more effective results. The intention of regularly updating colleagues is not to add to the burden of administrative reporting but to share ideas, successes and offer a platform for dialogue, requests for participant's input and help. These updates will be potentially a rich resource.

To initiate a structure for internal updating (and indeed all communications activity throughout the pilot's lifetime) it is proposed that each WP should nominate a member who will be a Communications Representative to act as the main liaison person for their group, and will be responsible for a two-way flow of information. A separate mailing list will be created for this new group coordinated by WP9 members.

9 Different channels and their benefits

There will be many overlapping areas between what CyberSec4Europe wants to communicate amongst its own partners and what it wants to broadcast externally, and often the platforms are the same.

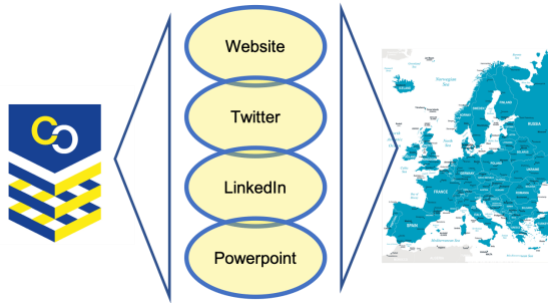

Figure 7: Internal and external channel overlap

The new CyberSec4Europe website will be the main platform to carry blog and video content, webinars, links to other social media etc for regular news contributions from each WP representative, bearing in mind that it is the project's shop window accessible by everyone from policymakers to the general public. Even if the website is mainly focussed on peer-to-peer dissemination, we have a responsibility to represent the project as clearly and dynamically as possible. The website has to tell coherent stories rather than just being a listing for results, publication and events, important though that information is.

There will also be a partners-only space on the new website for participants only, accessible by password, which can act as a communication forum to spread new ideas, results that are not ready to be publicly announced, requests for advice etc, privately within the consortium.

9.1.1 Twitter

CyberSec4Europe's Twitter account is growing healthily but has the potential to do more. It will spread the project's visibility much more effectively if all partners can follow @CyberSec4Europe both as individuals and from their organisational accounts, and re-tweet any @CyberSec4Europe posts as quickly as possible. Similarly, partners should alert WP9 about

any news/material that should be posted from the @ CyberSec4Europe feed. Each WP should aim to provide the material for a tweet on a monthly basis at a minimum.

9.1.2 YouTube

CyberSec4Europe has created a YouTube channel to host short films/interview/webinars on the project which partners will be expected to contribute to on a regular basis. As with other social media platforms, it will be beneficial if these can be shared by partners through all other channels as new content is added. These will also be linked to the main website.

9.1.3 CyberSec4Europe Blogs and LinkedIn

Partners will also be expected to produce blog content for the project website on a rotational basis (or more frequently if desired). Again, as these blogs will be in the public domain, there is a responsibility 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. These blogs can sign-post the audience to more high-level content, research papers etc. if the audience wants to deep-dive into technical issues. The website has to cater for a broad audience – the tone of the content has to reflect that.

The same considerations apply to CyberSec4Europe's LinkedIn page.

9.1.4 Managing social media channels

The effort of setting up and producing content for the various channels as described above can be further rewarded by the careful use of social media management tools such as Sprout Social or Hootsuite. These tools which can provide a more detailed level of analytics, track the progress of various conversations, plan our calendar of social content and multiply the reach of our various postings. WP9 will be selecting one of these tools over the next quarter to implement a more nuanced and powerful use of social media output, ensuring that CyberSec4Europe reaches the parts that others haven't!

9.2 A Communications Handbook

A handbook for communications will be produced for all partners outlining the various media available for communication and dissemination. It will offer advice and resources to help and all CyberSec4Europe partners, and WP leaders in particular, get their message across to as wide an audience as possible. It will also outline the project's procedures for fact-checking and advice on confidentiality issues. The handbook will be ready by M9.

9.3 Evaluation and feedback

It will be important to ascertain that the internal communications structures that the project has created are fit for purpose and that all participants know where to find news from colleagues, create and participate in conversations and commit to promoting their individual work areas as effectively as possible. It is proposed that all members will be surveyed by questionnaire at M12, M24, M36 to check the efficacy of the internal communications strategy, and that, if necessary, adjustments can be made in order to ensure that participants are not

simply working in their silos but have a comprehensive overview of their colleagues' progress in other work packages.

Partners will be incentivised to contribute to this information flow by a regular competition at each face-to-face project event to produce the most effective and creative presentation on their workpackage. These would be short sessions of 15 minutes in which participants can determine their best method of updating colleagues, for example by video presentation, animated presentations et al.

The narratives from the project are not predetermined and will not be static – they will develop as research results become clearer, new policy recommendations are shaped and new methodologies are established. The story from CyberSecurity4Europe will be ever-evolving, exciting and clearly communicated at all times to all levels of our multiple stakeholders.

10 The wider objectives of CyberSec4Europe and the other three pilots

CyberSec4Europe is one of four pilot projects (the others being CONCORDIA, ECHO, SPARTA) chosen to address the Horizon 2020 Cybersecurity call SU-ICT-03-2018. Each of the four projects has a different but complementary approach to the shared common goals, working together with Europe's cybersecurity eco-system to advance and strengthen the ways cybersecurity research, innovation and deployment are performed in Europe.

The four projects will cooperate and coordinate their activities extensively across the broad range of cybersecurity-related activities including demonstration test- and use-cases in eHealth, finance, telecommunications, smart cities and transportation. The use of cyber ranges, training and education programmes to tackle the cybersecurity skills gap in Europe will help deliver innovative marketable solutions, made in Europe, that will address the future cross-domain cybersecurity challenges to the security of the Digital Single Market.

These projects have been established to assist the EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence.

The strength of the four pilot projects is that they bring together over 160 partners, including large companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States and several Associated Countries. The overall EU investment in the projects is more than 63.5 MEUR.

Given this significant level of investment, it is important that all actors work cooperatively to assist in the promotion and impact of this research programme. This will ensure that the sum of these activities is even greater than its four constituent parts. This approach represents the greatest value to EU taxpayers and is a great opportunity for all researchers to form excellent collaborative partnerships and links. It will also significantly boost the profile of each individual pilot under a common "brand".

10.1 The Cybersecurity Competenence Network (CCN) Communications Group

To this end in early March 2019 the four pilots established a Communications Group which shares responsibility for defining and disseminating the joint message amongst the pilots.

The Communications Group meets regularly by monthly phone conferences, and by six-monthly face-to-face meetings, during the lifetime of the pilots to coordinate joint communications activities and develop the common unifying message in parallel. They will share ideas and approaches to ensure that best practice is determined and advanced, and that, ultimately, the widest possible audience are receiving the same message.

The CCN Communications Group of the four pilots has created an embryonic governance structure to determine how each pilot will work in sync with the rest of the group.

Each pilot's commnications lead will chair the group on a six months' rotational basis and oversee the coordination of planned activities during this six month cycle[3]. They have committed to meeting regularly by monthly phone conferences, and by six-monthly face-to-face meetings, during the lifetime of the pilots, to coordinate joint communications activities and develop the common unifying message in parallel. They will share ideas and approaches to ensure that best practice is determined and advanced, and that, ultimately, the widest possible audience are receiving the same message.

There will be natural synergies between the communications work that each pilot undertakes, and the therefore investment of time spent working together will benefit the work of each the individual pilots.

10.2 Early results

An over-arching brand **CyberCompetenceNetwork** has been created:

Figure 8: The four pilots' common logotype

[3] The first chair was CONCORDIA from March to June 2019. Future chairs are ECHO (July to December 2019), SPARTA (January to June 2020) and CyberSec4Europe (July to December 2020). From January 2021, the cycle begins again, indicating that, as it stands, CyberSec4Europe will not chair the group commencing July 2022, as the project is due to finish that month.

A common website has been designed and built and will undergo further development based on the agreed set of operational principles for the Communications Group.

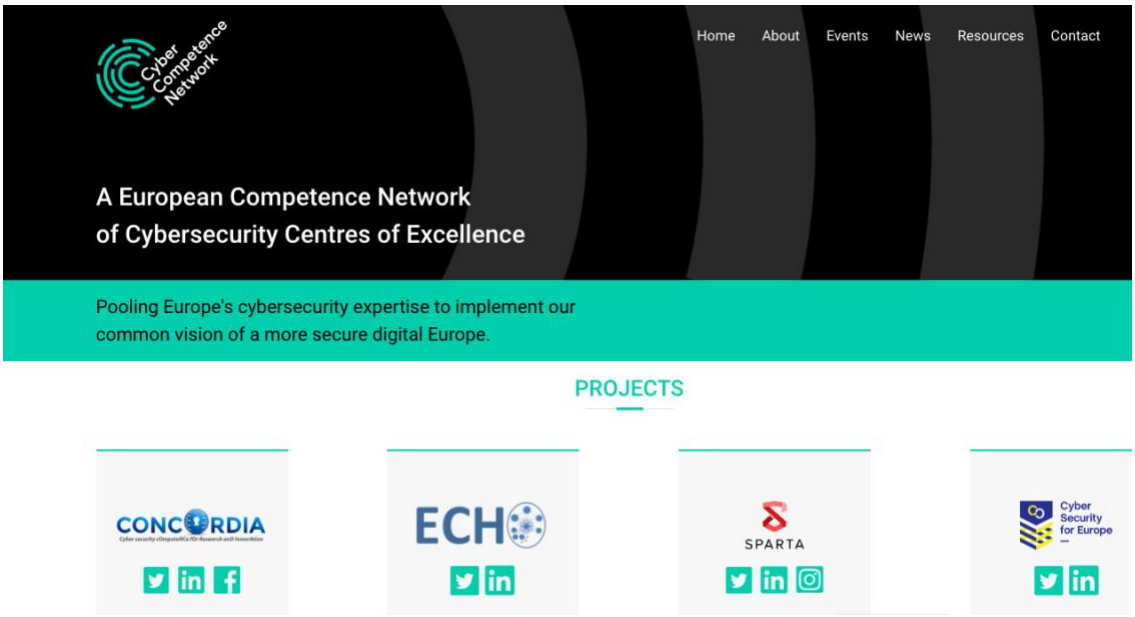

Figure 9: The four pilots' common website

The website provides information about events, publications and other activities as well as serving as a portal to each project's website and social media channels. It will be continuously developed in tandem with each pilot's own communication channels during the lifetime of the projects.

10.3 Future collaboration

The Communications Group will have a face to face meeting in M8/M9 to share salient aspects of each pilot's communications strategies in order to identify and map a way forward on areas of commonality.

Some early indications of potential synergies between pilots are:

- Federated cyber ranges.
- Early warning systems
- Certification and standardisation
- Education and training
- Face-to-face sessions with citizens

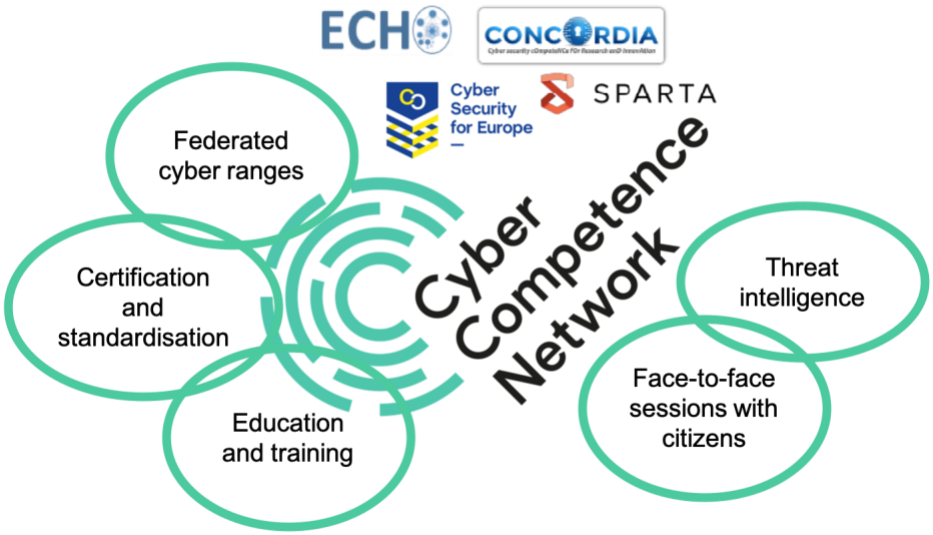

Figure 10: Areas of overlap and synergy between the four pilots

Although there is not yet an agreed consensus on how the four pilots, acting as a quasi-independent cluster, will operate and work together, there are a number of high level assumptions that can be posited at this stage.

- **Target audience:** European cybersecurity eco-system and general public
- **Messaging:**
  - A consistent high level set of pilot independent messages that can be used by each of the pilots
  - A set of two-three indicators of the individual flavours of each pilot that highlight the different approaches being taken
- **Tools and channels:**
  - **Common website:** The day-to-day management of the CCN website is carried out on a rotational basis by the current chair. The CCN website currently links to each individual pilot website and social media feeds;
  - **Events:** The website is intended to contain a listing of all events that are of relevance to all four of the pilots;
  - **Scientific publications:** The Commission has requested that the common website acts as a consolidated repository for all scientific publications from all four pilots;
  - **Social media:** The next face to face meeting will determine whether any common social media accounts should be created;
  - **Brand management:** The common brand was created on behalf of the Communications Group by CyberSec4Europe who will continue to manage the use and application of the logotype and the associated brand;

- **Blogging:** The Commission invited each of the four pilots to prepare a blog or news story to be posted on the Commission website. The intention was:
  - To promote our project, our team and our project ideas
  - To explain how and why our project will assist the EU in strengthening its cybersecurity and cyber resilience and/or our role in piloting the EU cybersecurity network
  - To inform about the next milestones for our project and according to our team what the challenges ahead are
  - The link with the other three pilots

  However, this activity seems to have stalled and it is now more likely that the Communications Group will develop its own;
- **Press releases:** The announcement of the launch of the four pilots at the end of February was coordinated in conjunction with DG CNECT with a series of press releases and synchronised social media activity. Going forward, CCN will issue press releases under the joint brand and a schedule for these releases will be determined shortly.

- **Co-representation:** The pilots have agreed that where possible, rather than send four representatives to an event, it should be possible to have a single representative who should represent the common CCN objectives as well as highlight the work of the other pilots.
  - This will reinforce the fact that the pilots are part of a greater whole, strengthen the CCN brand as well as spread news and information about what the other pilots are achieving.
  - A joint brochure and a common set of Powerpoint slides will be created in support of this initiative
- **Monitoring:** This includes:
  - Increase uptake of dissemination activities through analytics
  - Project impact and visibility in media
  - Media output of consortium partners

It should be apparent that there will be significant overlap between what each of the pilots do individually and what they present as a coordinated collaborative group. This will undoubtedly impact aspects of the CyberSec4Europe communication and dissemination planning outlined in this report.

11 Communications resources for project partners

The European Commission has a number of resources that can be accessed by project partners and it actively encourages projects to inform them about interesting topics, news and events in order to help raise profiles. In addition, several freely accessible tools are available and are described in the following sections.

11.1 Publications

Horizon Magazine

Horizon is the EU Research & Innovation e-magazine. It covers the latest developments in EU funded research and innovation, communicating the priorities and achievements of EU-funded research, its impact on citizens' lives and its contribution to the EU goals of smart and sustainable growth. It is written by independent journalists on behalf of DG Research & Innovation and is updated at least three times a week with new articles.

11.2 Project stories

Articles about selected EU-funded research projects, which led to breakthroughs, discoveries and world-firsts by taking great ideas from the lab to the market, at the same time contributing to economic growth and creating jobs, and tackling societal challenges.

research*eu results magazine

This print magazine features highlights from the EU-funded research and development projects. It is published 10 times per year in English, and covers mainly the research areas of biology and medicine, social sciences and humanities, energy and transport, environment and society, IT and telecommunications, industrial technologies and space.

research*eu focus

This print magazine covers in each issue a specific topic of research interest. It features articles on EU policies, initiatives, programmes and projects related to research and technological development and their exploitation. It is published at irregular intervals up to six times a year in English. Exceptionally, it may be available in other European languages as well.

To reach any of these outlets about any interesting project outcomes, the first step is to communicate with the project officer, which in turn would lead to contact from a journalist contracted by the European Commission.

11.3 Newsletters

Newsletters are published by the European Commission for different research areas.

11.4 Co-publications or editorial partnerships

The European Commission works with private publishers and international organisations to promote the dissemination of relevant publications. Scientific publications and books, including conference proceedings, may be co-published in this way.

11.5 Audiovisual

Futuris Magazine

Short documentary-style television magazine in various languages, appearing at least 22 times on the EuroNews channel throughout Europe. EuroNews has editorial independence, but we are in

contact with them to suggest good stories. Since it is television, this is interesting for visually appealing projects and demonstration activities.

11.6 Events

Events on the Commission's Research & Innovation website

This website displays research and innovation-related conferences and events. Events can be submitted by using the "Suggest an event" functionality available on the left-hand side of the website.

Events on the CORDIS website

This website displays researchrelated conferences and events. Submitting an event requires one-time registration on the CORDIS website Conferences and events organised by the European Commission Throughout the year, the European Commission (co-organises a variety of conferences, both in Brussels and elsewhere. These may include exhibition areas or sessions at which project work could be presented.

11.7 Open access scientific publishing

Openaire

The Open Access Infrastructure for Research in Europe is an electronic gateway for peer-reviewed articles and other important scientific publications (pre-prints or conference publications).

11.8 Online news

Headlines on the Commission's Research & Innovation website

Headlines report on recent developments in research and innovation in Europe and beyond and are devoted purely to projects. Suitable stories to be published on the site are selected on a daily basis.

CORDIS Wire

CORDIS Wire provides registered users with a simple interface to publish articles on the CORDIS website's News and Events service. All articles are moderated by CORDIS editors before publication.

12 Acknowledging EU funding – official guidelines.

Beneficiaries of the EU's Horizon 2020 research and innovation programme have the obligation to explicitly acknowledge that their action has received EU funding. This must be done, if possible and unless the Commission/Agency requests otherwise, in all communication, dissemination and IPR activities as well as on all equipment, infrastructure and major results funded by the grant.

The EU emblem and reference to EU funding must be displayed in a way that is easily visible for the public and with sufficient prominence (taking also into account the nature of the activity or object).

Examples: for equipment and major results a sticker or poster, for an infrastructure a plaque or billboard.

For all communication activities this should be done with the following statement:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830929.

For further information see:

https://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/acknowledge-funding_en.htm