D9.1

First exploitation and dissemination plan

WP9 – Exploitation, Dissemination, Communication and Standardization

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Due date of deliverable: 30/09/2017
Actual submission date: 30/09/2017

30/09/2017

Version 0.16

Responsible partner: DIGICAT
Editor: P.A. Galwas
E-mail address: paul.galwas@digicatpult.org.uk

Project co-funded by the European Commission within the Horizon 2020 Framework Programme

	Dissemination Level	
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Authors: P. Galwas (Digicat), G. Costantino (CNR), F. Di Cebro (SAP), J. Dobos (3D Repo), I.Matteucci (CNR), M. Shackleton (BT), L. Sobkowiak (GPS), C. Wong (3D Repo), C. Wright (Digicat)

Approved by: G. Costantino (CNR), I. Matteucci (CNR)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	13.01.2017	P.A. Galwas	DIGICAT	Initial draft of ToC for review
0.2	13.02.2017	P.A. Galwas	DIGICAT	Update following review
0.3	08.06.2017	P.A. Galwas	DIGICAT	Initial draft of plan for partner input and review
0.4	16/06/2017	G.Costantino, I. Matteucci	CNR	Publications list from CNR
0.5	20.06.2017	J. Dobos	3D Repo	Review of the whole doc plus 3D Repo section plus grammar
0.6	20.06.2017	M.Shackleton	BT	Review of the whole doc plus BT section plus grammar
0.7	20.06.2017	F. Di Cebro	SAP	Review of the whole doc plus SAP section
0.8	27.06.2017	P.A. Galwas	DIGICAT	Update following review
0.9	27.07.2017	C.Wright	DIGICAT	Adding further detail from partners
0.10	31.07.2017	P.A. Galwas	DIGICAT	Adding details on standardisation plan
0.11	18.08.2017	P.A. Galwas	DIGICAT	Prepare for review meeting
0.12	01.09.2017	P.A. Galwas	DIGICAT	Update following additions from BT, U. of
0.13	13.09.2017	I. Koparanova	HPE	Adding HPE section
0.14	19.09.2017	L. Sobkowiak	GPS	Adding Grid Pocket Systems section
0.15	19.09.2017	C. Wong	3D Repo	Proof read of whole document
0.16	21.09.2017	P.A. Galwas	DIGICAT	Update after review

Executive Summary

This is the first exploitation and dissemination plan for the C3ISP project. The document also contains a plan for exploitation and innovation, standardisation and communication.

The exploitation and innovation plans cover business scenarios and models, exploitation approach and plan, knowledge and intellectual property management and protection, and sustainability.

Individual exploitation plans from each partner focus on innovation aspects, and the research partners contribute plans on how to support third parties and industrial organisations that adopt and exploit the C3ISP results.

The standardisation plan outlines the approach to identify gaps in the current landscape and engagement with standard bodies.

The communication plan defines the communication objectives and approach, and lists planned publications and events.

Deliverables D9.2, D9.3 and D9.4 report on the exploitation and dissemination throughout the project against the plan in this document (D9.1).

Table of contents

1 Exploitation and Innovation

1.1 Mission statement

The mission of the C3ISP project is to define an exploitable collaborative and confidential information sharing, analysis and protection framework-as–a-service for cyber security management, regulated by Data Sharing Agreements (DSAs) that are computer interpretable and multi-stakeholder.

The framework seeks to share information inside a collaborative multi-domain environment to improve detection of cyber threats and response capabilities, while appropriately preserving the confidentiality of the shared information.

1.2 Industry state of the art

The project plans to identify and partition the industrial markets that are relevant to C3ISP exploitation, and to classify potential market sectors and stakeholders who could benefit commercially from the outcomes of C3ISP.

Here we summarise the essential parameters of this analysis to enabled sufficient refinement of the planning. As the project executes, the approach will be further developed and results summarised in the Exploitation and Dissemination Reports (D9.2, 9.3, & 9.4).

1.3 Business scenarios

The project plans to enumerate a set of business scenarios that constitute potential markets, each addressing a set of specific stakeholders through a specific channel.

Each business scenario will be represented by one of more business canvases, which will provide sufficient specificity to refine the associated propositions and business cases.

The business scenarios will be identified by considering the space containing:

- *Classes of Business Models*, such as one-side and two-sided markets
- *Classes of Stakeholders* in the context of Customer Segments
- *Classes of Channel*, including licensing, indirect sales, direct sales
- *Clusters of Value Propositions* that could derive from C3ISP capabilities and outcomes

1.3.1 Classes of business model

1.3.1.1 n-sided business models

Classes of business model include *one-sided business models* where the client pays directly for a benefit. In contrast, *two-sided business models* are when a benefit is provided to one class of client (possibly at no direct cost), while an associated benefit is provided to another (different) class of clients who pay. For example, a service provider (e.g., an ISP or cloud provider) may analyse threat intelligence from other ISPs and sell the result to an Enterprise.

There is also the possibility of a three-sided business model, for example where an SME provides threat intelligence (such as log data) to a service provider, who extracts (and possibly sells) information to other SMEs and (say) a national CERT.

1.3.1.2 Primary or secondary offering

The benefits derived from C3ISP outcomes could be a *secondary offering* – that is productised as additional capabilities or features to an existing, and potentially established, product or service; or as a stand-alone *primary offering*.

For example, C3ISP-enhanced Managed Security Service Provider (MSSP) could be bundled with cloud computing hosting, for a given market sector, such as SMEs; or enhanced MSSP could be offered as a separate service, e.g. to enterprise.

1.3.1.3 Aggregators

Another key consideration in the classes of potential business models centres around aggregation. The value of threat intelligence derived from analysis of input data is likely to increase significantly as the volume of that data increases. Therefore, there could be intrinsic business benefits in becoming an *aggregator* by accumulating threat data inputs. CERTS already do this, typically for the public good, but other companies could in principle seek to aggregate for advantage, as we have seen in businesses that support on-line advertising.

1.3.1.4 Intermediation

A business that can discriminate on the quality of its intelligence data, such as through aggregation, potentially could act as an *intermediator*, which seeks to 'broker' between suppliers of crude threat intelligence ('sellers') and consumers of refined TI ('buyers').

1.3.2 Classes of stakeholders

1.3.2.1 ISPs

Internet Service Providers (ISPs) could implement a more advanced Distributed Denial of Service (DDoS) prevention strategy exploiting the information coming in real time from a community of registrars, to improve reliability.

They could also perform preventive analysis for social engineering attacks such as Domain Hijacking, by being able to trigger timely action of law enforcement authorities, minimising the possible damage coming from these attacks.

1.3.2.2 Enterprise

Enterprises could gain value from using C3ISP outcomes directly in their systems, as well as indirectly when using 3rd party services, such as cloud hosting and business-level capabilities (e.g., Salesforce).

1.3.2.3 SMEs

Small and Medium-sized Enterprises (SMEs) could define through Data Sharing Agreements DSAs) which information they wish to share with which parties, such as CERTS, ISPs, and cloud hosting services. These parties could implement better services and offer threat intelligence to the SMEs and other stakeholders.

1.3.3 Classes of channel

Traditional channel models include:

- OEMing intellectual property, such as the rights to use patented technologies or, e.g., design for data sharing agreements, or software product licensees (e.g., for a component of the C3ISP architecture), for inclusion in the customer's products or services.

- Direct sales of a product or service to the end-user
- Indirect sales through a reseller, who for example can provide supporting capabilities.

Direct and indirect sales channels typically involve choices over the delivery method.

Where time-varying data such as threat intelligence is concerned, there is also the question of the relationship between the value and timeliness of a data feed. For example, trading data supplied to an automatic trading system is much more valuable than delayed trading data published on a consumer 'share price' web site.

1.3.4 Clusters of value propositions

It is valuable to consider clusters of value propositions, since it is likely that a given proposition may apply to more than one business model.

1.3.5 Developing business scenarios

As an initial stance, we plan to develop one business scenario to cover each pilot, then validate the scenario with stakeholders in the pilot, and based on the learnings from the pilot.

During the validation process, we will explore the feasibility of developing additional scenarios, by varying the classes of business models, channel, etc., using a methodology such as morphological boxes [1], [2], and SCAMPER [3].

Table 1 shows the form of morphological boxes.

Table 1 - Morphological boxes for business scenario development

	Configuration		
Parameter	**Scenario 1**	**Scenario 2**	**…**
n-sided business model			
Primary/secondary offering			
Aggregation?			
Intermediation?			
OEM/Direct/indirect			
Delivery method			
Timeliness?			
…			

SCAMPER encourages diversity by asking these questions:

- *Substitute?* Substitute people, components, materials
- *Combine?* Combine with other functions or things
- *Adapt?* Adapt functions or visual appearance
- *Modify?* Modify e.g. the size, shape, texture or acoustics
- *Eliminate?* Reduce, simplify, eliminate anything superfluous

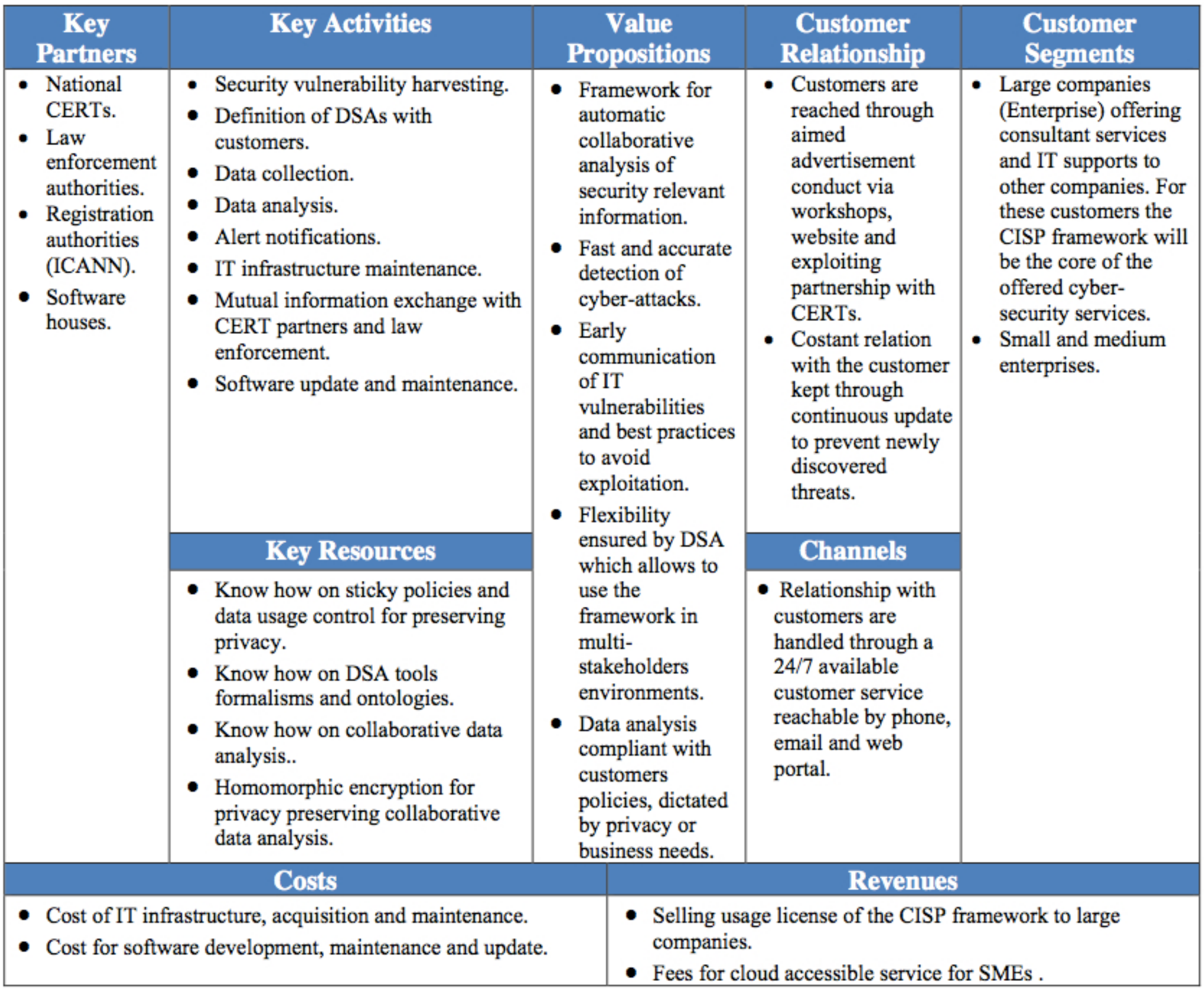
- *Reverse?* Use conversely, invert, reverse

Once an initial set of business scenarios have been developed working with pilots, they will be prioritised working with appropriate stakeholders in the context of open innovation workshops.

1.3.6 Detailing Business Scenarios

Each business scenario is presented according to the standard model canvas defined by Osterwalder and Pigneur [4], using the format shown in Table 2.

Table 2 - Template for Business canvas for scenario <n>



Key Partners	Key Activities	Value Propositions	Customer Relationship	Customer Segments
• National CERTs. • Law enforcement authorities. • Registration authorities (ICANN). • Software houses.	• Security vulnerability harvesting. • Definition of DSAs with customers. • Data collection. • Data analysis. • Alert notifications. • IT infrastructure maintenance. • Mutual information exchange with CERT partners and law enforcement. • Software update and maintenance.	• Framework for automatic collaborative analysis of security relevant information. • Fast and accurate detection of cyber-attacks. • Early communication of IT vulnerabilities and best practices to avoid exploitation. • Flexibility ensured by DSA which allows to use the framework in multi-stakeholders environments. • Data analysis compliant with customers policies, dictated by privacy or business needs.	• Customers are reached through aimed advertisement conduct via workshops, website and exploiting partnership with CERTs. • Costant relation with the customer kept through continuous update to prevent newly discovered threats.	• Large companies (Enterprise) offering consultant services and IT supports to other companies. For these customers the CISP framework will be the core of the offered cyber-security services. • Small and medium enterprises.
	Key Resources		**Channels**	
	• Know how on sticky policies and data usage control for preserving privacy. • Know how on DSA tools formalisms and ontologies. • Know how on collaborative data analysis.. • Homomorphic encryption for privacy preserving collaborative data analysis.		• Relationship with customers are handled through a 24/7 available customer service reachable by phone, email and web portal.	

Costs	Revenues
• Cost of IT infrastructure, acquisition and maintenance. • Cost for software development, maintenance and update.	• Selling usage license of the CISP framework to large companies. • Fees for cloud accessible service for SMEs .

1.4 Business model

For the set of priority business scenarios, we will develop detailed business models, including strategy for investment and outline roadmap.

As these business models are refined, it may be possible to identify clusters of characteristics, which will allow optimisation of the development of core C3ISP technologies or components.

1.4.1 Market analysis

To supplement the business model, a market analysis will be generated appropriate to the market segments identified in the priority business scenarios.

Market analysis will consider these aspects for each business case:

- Business case(s)
- Value propositions
- Shared capabilities
- Channels
- Support
- 3rd parties
- Industrial organisations

1.5 Exploitation plan

1.5.1 Exploitation Board

An *Exploitation Board* consisting of the research and industrial user partners will be established to coordinate exploitation actions for the project.

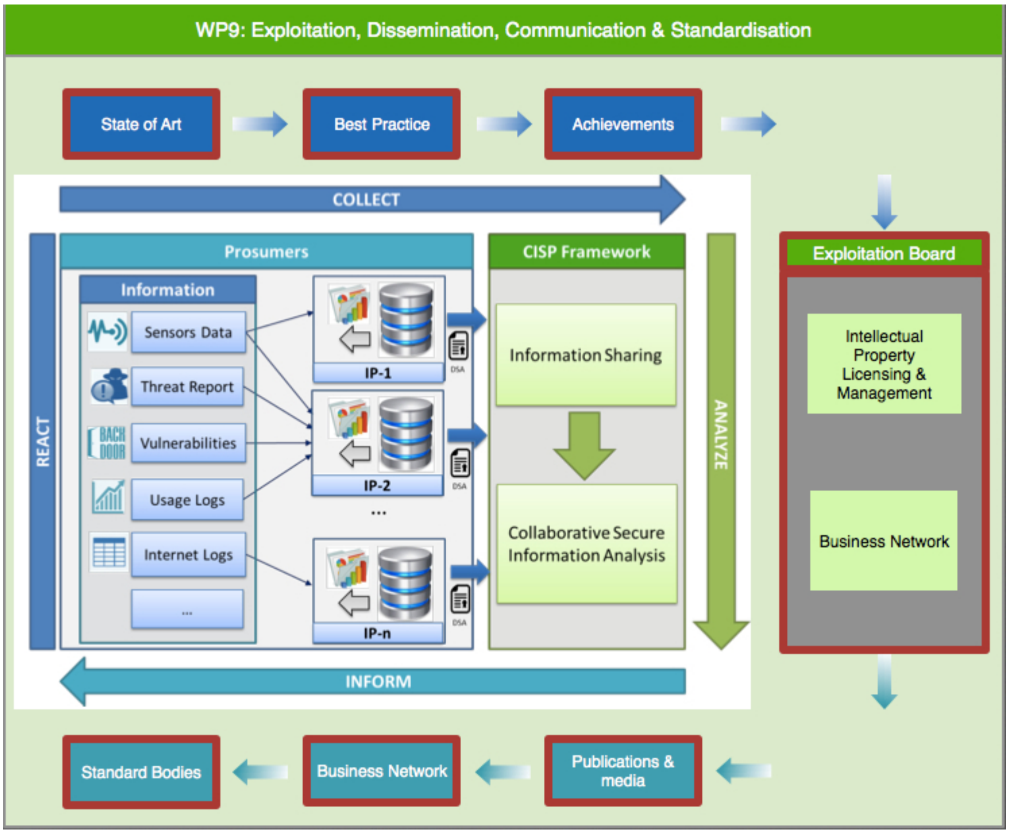


Figure 1: The Exploitation Board in context of the project

State-of-the-Art from research and industrial perspectives is described in the Exploitation and Dissemination Reports. As the project advances, C3ISP achievements and recommendations

[1] http://www.csoonline.com/article/3047197/techology-business/researching-the-threat-intelligence-space.html

for best practices will be identified, and fed into the Exploitation Board, together with the context of the Business models.

The Exploitation Board prioritizes intellectual property that should be protected, and identifies licensing mechanisms that need to be in place to protect that intellectual property and for commercialisation.

The Exploitation Board also consults indirectly with the Business Network to refine the business model, and feeds findings and recommendations, by disseminating through publications, across the business network, and the media.

In particular, the open innovation workshops will invite participants from the consortium members' Business Networks who are selected to suit the needs of each particular workshop.

1.5.2 Identifying potential Exploitation Board Members

The process of selection of the members of the Exploitation Board is open and transparent process:

1. Digital Catapult liaises with representatives of all the consortium organisations to identify optimal Exploitation Board participation.
2. Each partner identifies suitable experts for the Exploitation Board role, through personal and industry networks, with the aim of establishing an initial list of experts for consideration by the consortium as a whole.
3. Compile all nominations in an excel file shared through SVN, recording the following information was recorded:
    - Expert's name
    - Expert's Organisation
    - Expertise
    - Country
    - Classification

4. Steering Committee reviews and agrees the list of experts (*Nominated Exploitation Board members*) to be contacted from the individual contributions, with members having opportunity to argue for or against the appropriateness of nominated members. The target size is one member from each Partner, complemented by and 2 or 3 external members.
5. The Project Coordinator formally invites Nominated Exploitation Board members. This formal invitation included the Exploitation Board Agreement. In order to formalise the agreement, the Members are asked to sign and return the agreement, which was then countersigned by the Project Coordinator, acting on behalf of the Consortium.

An example of this formal invitation (e-mail) can be seen in Section (1.5.4) and the Agreement in Section (0). We will e-mail nominated members and record status and a version of the final e-mail D9.2 etc.

1.5.3 Meetings of the Exploitation Board

The Exploitation Board will be aligned with the specific needs of the project. The Board can meet with C3ISP as a whole, in specific configurations (e.g. according to stakeholder groups), as a group of members and as a single member.

The Project Manager will notify Exploitation Board Members of a meeting at least one month in advance, and we will supply meeting documents by email to Exploitation Board Members at least one week before the associated meeting.

The first face-to-face Exploitation Board meeting is proposed for Q1 2018. The Coordinator will write the minutes of the Exploitation Board meetings, and prepare the implementation of the Exploitation Board's suggestions.

1.5.4 [DRAFT] Email to Exploitation Board Members

From: Cherlaine Wright [Cherlaine.Wright@digicatapult.org.uk]
Sent: <date>
To: <name>
Subject: Exploitation Board: C3ISP project

Dear <name>,

I hope you're well.

I'm Cherlaine Wright, the Project Manager for C3ISP here at the Digital Catapult. It's great news that you're able to partake in the Exploitation Board and we are delighted to have your support.

Attached you will find an Invitation and agreement to join the Exploitation Board of the C3ISP Project. Within you will see details of various activities you could be asked to support, but as Kathryn has rightly confirmed all are subject to mutual agreement and availability.

Please can you populate the highlighted fields, scan and return to me at your earliest convenience.

If you have any questions, please don't hesitate to ask.

I look forward to meeting with you in the future

Best Regards,

Cherlaine

Project Manager

M: +44 (0)7796 950995

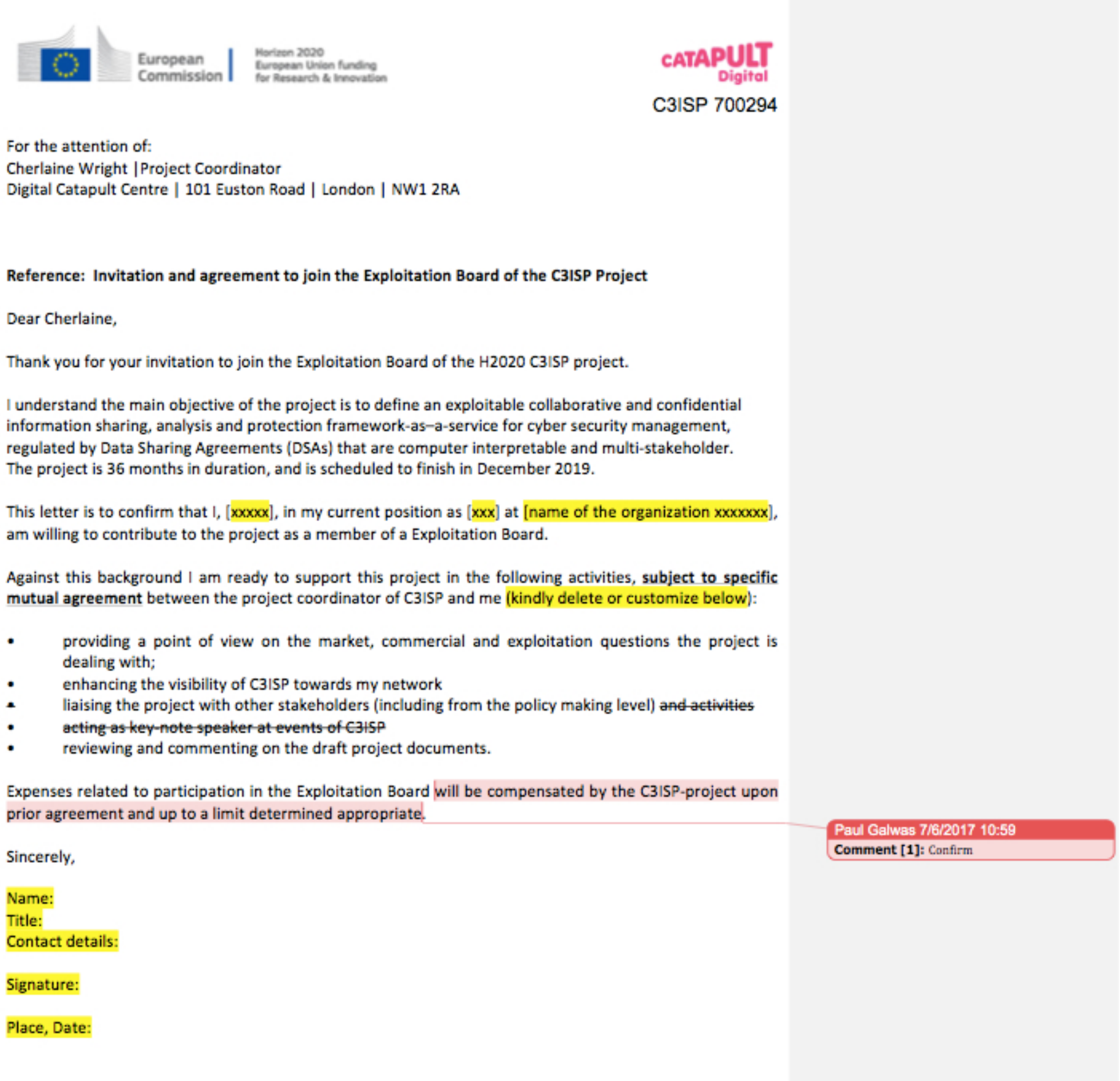
Digital Catapult Centre | 101 Euston Road | London | NW1 2RA

www.digitalcatapultcentre.org.uk

@DigiCatapult - LinkedIn

Figure 2: Text of an e-mail to Nominated Exploitation Board Members

1.5.1 [DRAFT] Exploitation Board Agreement



C3ISP 700294

For the attention of:
Cherlaine Wright |Project Coordinator
Digital Catapult Centre | 101 Euston Road | London | NW1 2RA

Reference: Invitation and agreement to join the Exploitation Board of the C3ISP Project

Dear Cherlaine,

Thank you for your invitation to join the Exploitation Board of the H2020 C3ISP project.

I understand the main objective of the project is to define an exploitable collaborative and confidential information sharing, analysis and protection framework-as–a-service for cyber security management, regulated by Data Sharing Agreements (DSAs) that are computer interpretable and multi-stakeholder. The project is 36 months in duration, and is scheduled to finish in December 2019.

This letter is to confirm that I, [xxxxx], in my current position as [xxx] at [name of the organization xxxxxxx], am willing to contribute to the project as a member of a Exploitation Board.

Against this background I am ready to support this project in the following activities, **subject to specific mutual agreement** between the project coordinator of C3ISP and me (kindly delete or customize below):

- providing a point of view on the market, commercial and exploitation questions the project is dealing with;
- enhancing the visibility of C3ISP towards my network
- liaising the project with other stakeholders (including from the policy making level) ~~and activities~~
- ~~acting as key-note speaker at events of C3ISP~~
- reviewing and commenting on the draft project documents.

Expenses related to participation in the Exploitation Board will be compensated by the C3ISP-project upon prior agreement and up to a limit determined appropriate.

Paul Galwas 7/6/2017 10:59
Comment [1]: Confirm

Sincerely,

Name:
Title:
Contact details:

Signature:

Place, Date:

Figure 3: Text of the Exploitation Board Agreement

1.6 Exploitation approach

This section summarises the methodological approaches taken to exploitation.

There are three cyclical processes applied throughout the project, each described in the following sub-sections.

1.6.1 Operating principles

The project will regularly perform assessments of the added value of C3ISP results against the industry and research state-of-the-art at the project meetings and, in the case of urgent events *ad hoc*. The findings from the assessments will be recorded in the Exploitation and Dissemination Reports (D9.2, D9.3, D9.4).

Where a change of plan is indicated, the finding will be fed into the agile refinement cycle.

1.6.2 Exploitation innovation

In order to increase business and innovation opportunities and investments criteria, and using the Digital Catapult's Innovation Services Pitstop ™ open innovation framework, we will seek to identify and explore suitable market sectors and business models where there is likely to be the greatest need and opportunity for the commercial exploitation of C3ISP. We will do this through the following interventions.

The first phase is to *understand* the market sectors. In consultation with the whole consortium we will identify which market sector business scenarios present the biggest need and commercial opportunity for further development of the C3ISP protection framework.

The second stage is to *validate and prioritise* those market sectors and business scenarios identified during the 'understand' phase, with a specially selected target audience to ensure the propositions meet the needs of the market.

1.6.3 Agile refinement cycle

Each of these phases, and starting from the very early stages of the development, will use an iterative innovation process comprising of a series of cyclical activities will be planned to mature the business case and appropriate agreements with all kind of partners will be established to commercially exploit any business opportunity, as shown in Figure 4.

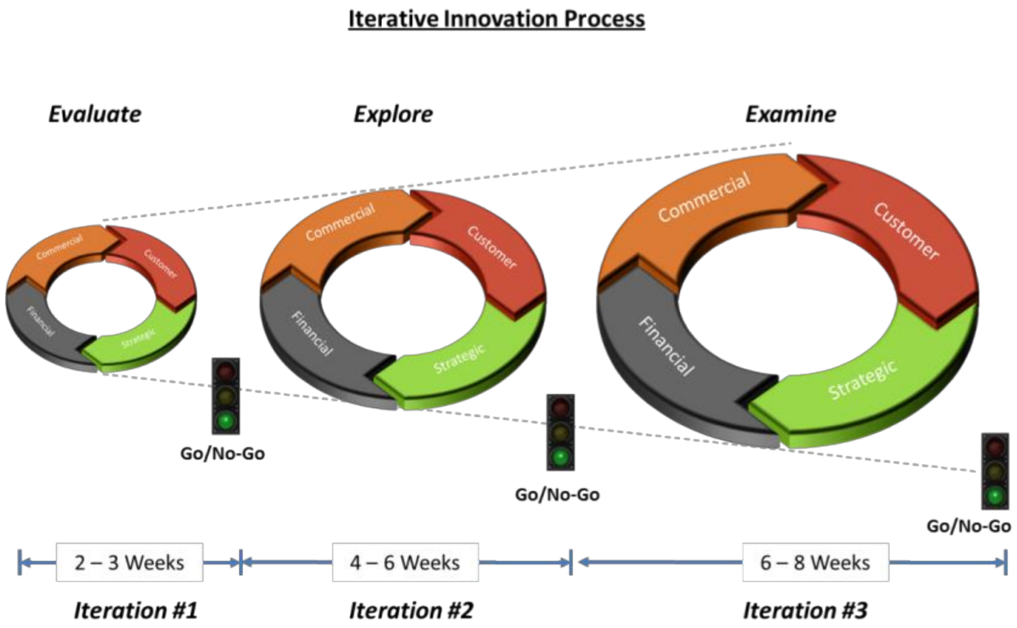


Figure 4: **Iterative innovation process**

The process will examine the Strategic, Customer, Commercial, and Financial themes separately.

1.7 Business network

1.7.1 Kind of stakeholder organisation

Table 3 shows the initial list[2] of the kinds of stakeholder organisation that cover the potential users, customers and other interested parties for C3ISP outcomes.

Table 3 - Initial list of kinds of organisation

Kind of organisation
CERT
City
Consortium
Enterprise
Government Body
ISP
Law Enforcement Agency
Public Authority
SME
Standard body

Table 4 shows the initial list of kinds of activity that party associated with an organisation could perform.

[2] Items that are struck-through (like ~~this~~) are included in this version for completeness, but expect to be omitted in the final version of the document.

Table 4 - Initial list of activities performed by parties

Kind of activity
advise
buy
disseminate
make policy
manage
own
partner
prospect
regulate
represent Organisations
supply

1.7.2 Community building

Consortium partners all contribute to the building of a business community against which assumptions can be validated and findings and recommendations propagated. Such Business Networks include specifically:

- Consortiums of other Horizon 2020 projects
- TRUESSEC.eu network
- Companies, researchers and individuals specifically selected for open innovation
- Leveraging each Partner's individual communities.

1.8 Individual exploitation strategy

This section summarises the exploitation strategy for each Consortium Partner.

1.8.1 BT

BT will leverage C3ISP outcomes into its own Cyber Security offerings and protection of customers on its cloud offerings. BT is aware of the challenges faced by SMEs in terms of cost sensitivity and limited ability to cope with complex security solutions. This is why the proposed solution in C3ISP is to create a federation of SMEs, in which each SME shares its experience into the common knowledge built up with the others, in a collaborative and confidential fashion, to face threats in a timely manner, as if the conglomeration of SMEs were a single company with enough resources to deal with them. BT's experience in combining security solutions together with Cloud technologies will prove useful here. As for some other consortium partners, BT has extensive expertise in commercialising cloud accessible services like C3ISP and the whole consortium will benefit from this capability.

BT is also a major MSS Provider, so can add value by providing a service wrap, tailoring the platform for a particular type of customer and/or market segment and brings the service to market. It is anticipated that successful validation of the technology in the Enterprise pilot would be followed by implementation in a BT enterprise cyber-defence MSS platform to enhance BT's offerings in this space. C3ISP will enable BT to define and develop a customer and incident centric method of integrating Cloud-based and Cloud-oriented branch of BT Security/Assure portfolio where Cloud-based data security services will be enforceable on private and public Cloud platforms in relevant vertical market sectors. BT's security and risk management services portfolio is known as BT Assure (although it is undergoing rebranding currently); it includes managed security services for DDoS protection, next generation firewall, web security, mail protection, cyber defence, data protection, identity and access solutions, etc. All these solutions are tailored to provide business continuity and to protect corporate assets and critical national infrastructures. The security portfolio provided by BT Global Services is primarily targeted at corporate and public organisations. The public verticals include central government, defence and security, health, home affairs and police and local government. The corporate sector mainly includes automotive, construction, consumer packaged goods, logistics, manufacturing, mining, oil and gas, pharmaceutical, retails, systems integrators, transport, utilities, financial markets, insurance, retail and private banking and wholesale banking and payments.

BT will also make use of major events to encourage both dissemination and exploitation. For example, it has already featured C3ISP progress and innovations at Innovation 2017 in June'17 at its global R&D HQ at Adastral Park. The event had 5000+ visitors, which included external customers, BT market-facing units, technologists, as well Press and Analysts.

1.8.2 CNR

The exploitation strategy of CNR is oriented to improve its research activities by taking advantages of the results and technologies that will be the provided as results of the C3ISP project. The main interests are related to the research topics linked to access and usage control policy, data sharing agreement, definition and translation of policy languages that will allow a customer to specify policies to different abstraction level. All these research streams are crucial to attract new business and scientific partners and collaboration for both new European project as well as for industrial activities.

1.8.3 Digital Catapult

Based on the findings of the C3ISP project, Digital Catapult seeks to identify and explore business models for a computer interpretable, multi-stakeholder, collaborative and confidential protection framework-as-a-service (*'protection framework'*). We plan to do this in the following ways:

- Identify potential new market sectors
- Explore possible business models
- Feedback findings to the market

Digital Catapult will seek to work closely with the consortium partners to undertake this activity. In consultation with the C3ISP partners:

- We will identify which market sectors present the biggest need and commercial opportunity for the development of the protection framework.
- We will then test these assumptions with the identified market sectors with a view to understanding the potential value propositions.
- We will then engage the partners corresponding ecosystems to refine findings, create business canvases and promote adoption of the C3ISP framework.

1.8.4 GridPocket Systems

As an SME company that provides large scale measurement and analysis of power, gas and water consumption, we are very interested in providing well secured software to the market. We aim to deploy all methods and technologies designed by C3ISP as a part of our Powervas system. GridPocket will test all created functionality of C3ISP project to be sure that all features are fully functional. After that GridPocket will try to deploy C3ISP functions to our customers systems that Powervas will share data with. During the life of a project GridPocket will deploy all C3ISP prosumer side components to our OVH cloud to protect our systems and get data from them to protect other C3ISP prosumers. GridPocket can provide to C3ISP data from routers, web servers logs, couple of types of APIs, databases (noSQL, MongoDB) logs, measurement devices and also logs and data from our Live Monitoring System that stores data about using resources of all components of our systems.

Gridpocket is going to build company internal policies that will be essential for running C3ISP in our company. GPS will also advise to our customers how to become compatible and inter operative with C3ISP.

1.8.5 HPE

HPE is a leader in IT and security solutions with its HPE Pointnext consulting business unit (https://www.hpe.com/emea_europe/en/services.html). HPE is also a market leader in cloud computing and hybrid cloud technologies. The interest of HPE in the project is in the commingling of the two worlds of cloud and security, being able to provide high added-value security services to the cloud offering, democratising security solutions and technologies, making them reachable and affordable also to small and medium enterprises. HPE deals with several customers interested in security products and services for their business, ranging from corporate customers, to cloud providers, to SME.

Cloud28+ (https://www.cloud28plus.com/) - an HPE initiative launched back in 2014 - is the largest worldwide ecosystem of cloud practitioners ranging from cloud providers, ISV, system integrators, consultancy firms, legal firms, etc. Being the Cloud28+ a partners' community, the need for governing a secure privacy-aware data exchange is of high interest. A secure collaborative approach for cyber threat information data exchange is relevant to provide a competitive advantage to all the federated partners. Leveraging on the high number of community partners (more than 500 worldwide), C3ISP solution could provide high benefit by enabling the development of cyber security detection services that takes into account the privacy protection of each federated member.

HPE also manages a Technology Showroom in Milano (Italy), an environment where top Italian customers are invited to experience the most relevant and innovative HPE technology, so we will have the opportunity to include C3ISP in our demonstrations. HPE is also setting up a Demo Centre in Firenze, in collaboration with national academic partners; we plan to include a C3ISP demo environment also in this initiative to showcase to interested customers and partners.

1.8.6 SAP

As an important player in today's market, SAP is concerned about the security of its operations together with peer organisations. SPA joined cyber-security intelligence sharing initiatives like Cyber Security Sharing & Analytics (CSSA) [5] to counter threats by leveraging on the collaboration among different stakeholders, exactly as for the C3ISP vision. CSSA is a European initiative whose members are among the most important EU industrial players (Airbus, Siemens, Bosch, Basf, BMW, Deutsche Telekom…). Its members share CTIs that are then consumed by the Security Operation Centres of the other partners.

SAP has therefore an important interest in C3ISP concepts and contributions in order to progress the state of the art in the practice of cyber threat information sharing and analysis. A natural exploitation of C3ISP results may be represented by cross-fertilisation activities in CSSA. The need to bring automation in CTI reporting and analysis is real, as well as the desire to create liaisons with other entities and communities, to enhance the amount of available data and therefore the quality of findings.

Another point of potential impact is represented by the influence of C3ISP concepts in SAP Tools. SAP Enterprise Threat Detection (ETD) [6], for example, is a tool that can be used to collect security events and context information as well as to monitor and to analyse events and alerts in SAP systems. In such a context, multiple C3ISP concepts may find a fertile ground for their reception. An initiative in this direction is represented by a number of proof-of-concepts of the C3ISP-developed differential privacy algorithms to ETD use cases. The initial feedback received a certain praise worth of being explored further in the development of the project. A part of these activities had also been showcased in the context of D-KOM, the annual meeting of the SAP developers' community and in a joint demo with BT.

1.8.7 Partner 3D Repo Ltd

As a provider of online tools for collaboration on 2D Geographical Information Systems (GIS) and 3D Building Information Modelling (BIM) in the cloud, 3D Repo is seeking the best possible cyber security solutions for their clients. These include large national-scale infrastructure projects, such as railways and highways, as well as potential future work on projects for the Ministry of Justice and Ministry of Defence in the UK and also across the rest of Europe. Therefore, having suitable monitoring and sharing infrastructure in place to prevent malicious activity on our servers is of paramount importance. We believe that the results of this project will be directly deployable with some of our largest customers, such as, Balfour Beatty, Crossrail and High Speed Rail 2.

3D Repo plans to:

1. Test and deploy initial prototype implementation of the C3ISP framework on 3D Repo's development servers on Rackspace
2. Integrate with BT Intelligent Cloud Protection infrastructure and deploy this solution with select customers for alpha testing
3. Evaluate the scalability of the solution in a production deployment with one large international client
4. Enter legal framework agreements and negotiate the commercial arrangements for exploitation in real-world scenarios
5. Fully commercialise this novel technology and bring it to market

1.8.8 University of Kent

The University of Kent is working closely with BT to add the C3ISP enhancements to BT's cloud systems. Exploitation by Kent during the life of the C3ISP project will take place in close cooperation with BT, but after the project finishes, BT will continue the exploitation on its own as described above.

1.8.9 CHINO

Security is a key aspect for CHINO company and service offering to SMEs and large enterprises in the digital health sector. To deliver high quality and secure services to its customers CHINO relies on state of the art security technologies, protocols and standards. CHINO considers security as a fundamental requirement in in its service design, and as an added value for its customers.

The mechanisms, tools and concepts developed in the C3ISP projects will be exploited by the CHINO company in the following ways:

- Test and deploy the C3ISP prototype within its sandbox computing environment which is used by CHINO customers in the integration phases (when real sensitive data are not managed and stored via CHINO API).
- Test the efficiency and effectiveness of the deployment in improving the CHINO service quality and security.
- Define and implement a communication strategy which uses the C3ISP technology and benefits to increase its trust and brand reputation. These are fundamental aspects for CHINO company and key to its success.
- Overall C3ISP project will deliver to the CHINO team the expertise and knowledge on the cyber security strategies and best practices applied by partners in current cloud technologies.

1.8.10 CEA

CEA exploitation strategy is twofold. On one hand will promote the practicality of homomorphic crypto-computing technology via the concrete results obtained on the pilots during the project (from one-to-one actions to the possible organization of workshops with interested industrial prospects). On the other hand, will manage the technology transfer towards either a spin-off or an existing private sector actor for commercial exploitation.

1.9 Research and IP state of the art

The reports D9.2-9.4 will summarise research and intellectual property state of the art in these main areas, as well as relevant adjacent areas as the analysis may indicate:

- Data Sharing Agreements
- Data Usage Control
- Collaborative cyber security information management
- Data analytics techniques
- Anonymisation techniques
- Homomorphic computing
- Visualisation techniques
- Managed Security Services

1.10 Background prior art

This section lists each Partner’s background IP that may be relevant to the C3ISP project.

1.10.1 BT

BT has existing capabilities in Visualisation (Visual Analytics) as well as Managed Security Services, which will be drawn upon as component technologies within C3ISP.

BT Visual Analytics is an in-house developed software suite which allows end users to rapidly create bespoke filters and rich interactive visualizations on a set of configured data sources. Machine learning, such as clustering, is used to elicit patterns that exist in the data and offer visual suggestions to analysts and allow them a toolset to conduct further analysis. It supports exploratory data analysis of a wide range of data and has been applied for several large-scale applications, including cyber security.

BT already provides a variety of security services to enterprise customers, including ones such as BT Assure Cyber and BT Assure Threat Monitoring that involve analysis of security-related data from customer networks. However, the threat is evolving all the time and the market is very competitive, so continual improvement of the services is necessary to remain competitive. The aim is to use C3ISP results to improve the service (e.g., by detecting more attacks, providing more information about them and eliminating false positives) in return for permission to pool data while providing assurances that sensitive information will not be revealed to third parties.

1.10.2 3D Repo

Prior to this Horizon2020 funded project, 3D Repo collaborated on Trusted Cloud High Impact Initiative project with BT under the EIT Digital funding scheme. Results of this collaboration have been published in a white paper *“3D Repo in a Secure Cloud Environment; a Case study*” [7], which is available online at: http://3drepo.org/projects/3d-repo-in-a-secure-cloud-environment-a-case-study/

3D Repo trademarked the text phrase *“British Information Modelling”* and *“BIM Forensics”* in the UK.

1.11 IPR protection

1.11.1 Patent, copyright, etc

The Consortium will from time to time identify areas of IP that it seeks to protect, and will decide to apply one of more IPR protection methods, including:

- filing a US Provisional Patent, which provides a priority date and can be followed by a full patent application within a year
- filing a Patent Cooperation Treaty (PTC) patent application, with later execution in nominated jurisdictions in the National Phase
- declaring copyright, by displaying, and where appropriate requiring under the terms of a license, the copyright notice: © <year> C3ISP Consortium
- protection under legal contract (rather than the above IPR protection means)

We currently believe that it is unlikely that any IP will be held as a Trade Secret, or protected as EU Design or Database rights.

1.11.2 Open access

The Consortium may explicitly designate certain IP for open access. In particular, the Consortium will follow the so-called 'green' open access for the scientific publications, which means that the published article or the final peer-reviewed manuscript is archived by the researcher - or a representative - in an online repository before, after or alongside its publication.

1.11.3 Licensing

The Consortium Parties may inform each other (according to Art. 25 Grant Agreement) and agree on a separate contractual arrangement to regulate limited license rights to Software on a royalty-free basis for implementation of the Project with one or more specified Party/ies. The Parties concerned will conclude this separate arrangement at any time they see fit within the timeframe of the Project.

1.11.4 Approach

The process for prioritising and applying IPR protection is as follows:

1. Identify an *IP Item* – a concept and associated set of artifacts as potential IP
   - It may be necessary to split one initial item into multiple IP Items
2. Assess the relative potential opportunity of the IP Item in terms of, by these attributes
   - Potential *market* size and lifetime
   - Degree of *differentiation* including scope, defensibility and degree of competition
3. Assess the *patentability*, including consideration of
   - Whether the on-sale bar has been breached
   - Sufficiency of novelty and non-obviousness
4. Identify effective means of IPR protection
5. Prioritise each IP Idea to action protective means, while seeking to establish a 'mesh' of IP protection from the growing set of C3ISP IP.

The Consortium may decide that some IP Items will not for explicitly protected, and other IP may be freely licenced, and made available through open access.

1.11.5 Knowledge collection and curation

The C3ISP SVN[3] is used to store all project data. The core deliverables will be used to index all substantive knowledge, and to document it or reference external documentation (such as papers) as appropriate.

The Exploitation Reports (D9.2-4) will include a schedule of IP Items, and an associated audit log of execution of IP protection process.

1.11.6 Intellectual Property identification and handling

The following are candidate domains for foreground IP:

- DSA Adapter
- Homographic encryption techniques
- Anonymisation techniques
- Information analytics Infrastructure

[3] Apache Subversion (often abbreviated as SVN) is a software versioning and revision control system.

Visualization of security level for sensitive information through security visualization tools.

1.11.7 Exploitation Board

The exploitation board (see above) may periodically suggest that topic is considered for protection as foreground IP.

1.11.8 Conflict management

The Consortium Agreement includes provision for conflict management.

1.12 Sustainability plan

The Exploitation Reports (D9.2-4) will describe a sustainability plan for the continued impact from project outcomes, including:

- Summaries of scenarios
- Analysis of options to differentiate and prioritize scenarios
- Approach to technology transfer.

2 Standardisation

The project will seek to impact international standardisation activities, through influencing domain specific initiatives on the topics relevant to C3ISP.

In order to provide meaningful contributions to the international standardisation landscape, C3ISP has a set of localised best practices based on the technical outcomes from the project and also the experiences from the pilots.

For efficiency, there will be a clear strategy and methodological approach for orchestrating C3ISP's contributions to influence standards/technical recommendations bodies:

1. Gap analysis of standard status and requirements
2. Prioritised engagement on specific standards with the associated standard body
3. Liaison with the standard body to recommend development of new standards or to support specific evolution of existing ones.

2.1 Standard state-of-the-art

An ENISA report [8] published gives a good summary of the evolution and the state in late 2014 of the standards and tools for the sharing of actionable information in the context of national and governmental CERTs, covering some 53 different standards and their inter-relationship, tracing their heritage back to the 1990s.

It also noted relevant standards that are no longer relevant, those not used in practice, as well as those under development, such as Intrusion Detection Extensible Alert (IDEA), which is now almost definitive [9], and Data Harmonization Ontology [10] for sharing abuse and vulnerability information.

The report also examined 16 information management tools, including those supporting analysis, but it did not specifically consider data analysis and visualisation standards applied to threat intelligence.

In addition to the domain of sharing and analysing threat intelligence, C3ISP uses of technologies such as access control, data sharing licences and privacy enhancing technologies and cryptography. Most of the associated standards are generic, so the project will seek to leverage them where appropriate.

It is possible that the project will discover particular requirements of sharing threat intelligence that will lead to making recommendations to develop existing standards in this space, or develop new ones. The approach described below allows for such possibilities.

2.2 Evaluate standards landscape

2.2.1 Gap analysis

Throughout the project, consortium members will regularly monitor evolutions and gaps in the relevant standardisation landscape, e.g. to identify new/incubation standardisation initiatives relevant to C3ISP.

They will report relevant findings and recommended at the project meetings and, in the case of urgent events *ad hoc*. The findings from the assessments will be recorded in the Exploitation and Dissemination Reports (D9.2, D9.3, D9.4).

2.2.2 Engagement

When appropriate, the project meeting will recommend deeper engagement with the appropriate standard body around a specific topic area.

Exploitation and Dissemination Reports (D9.2, D9.3, D9.4) will record the engagement with individual standard bodies, with a view to seek deeper understanding of a given standard domain, influence the evolution of a standard, or suggesting and promoting the development of a new standard.

2.3 Contribution to & liaison with standard bodies

When agreed by the Consortium, the project will cooperate closely with existing standardisation bodies on specific topics that are key to the project or its exploitation.

Those partners undertaking specific engagements with standard bodies will initially report their activities to the consortium at least at the next project meeting. In addition, the Exploitation and Dissemination Reports (D9.2, D9.3, D9.4) will record the evolution of progress.

The project has initially prioritised engagement with OASIS.

2.4 Conclusion

The last Exploitation and Dissemination Reports (D9.4) will summarise the project's standardisation activities, conclusions and recommendations so that the project partners, and any future projects, can continue this standardisation work.

3 Dissemination and Communications

3.1 Communications objectives

3.1.1 Communications objectives

There are two major communications objectives:

- Raise awareness of C3ISP project and mission, primarily to encourage contribution to validate and refine the business opportunities and dissemination approach.
- Disseminate C3ISP outputs in both the commercial and research domains.

3.1.2 Positioning

C3ISP is a collaborative EU Horizon 2020 research project that seeks to advance the Technological Readiness Level (TRL) of core technologies that protect confidentiality for analytics of sensitive data. It makes the research concrete through pilots that analysis shared threat intelligence information.

3.1.3 Target audiences

The target audiences are:

- Providers of aggregated security services, including CERTS
- Providers of computer services (ISPs, cloud service providers (IaaS, AaaS))
- Companies who seek to protect their computing capabilities, products and services, specifically enterprises and SMEs
- Providers of security products and services who could license C3ISP outcomes to improve their security or privacy capabilities
- Security and privacy researchers who seek to advance the state of the art
- Standard and policy bodies who might relate to C3ISP recommendations
- EU project stakeholders

3.1.4 Desired actions

During the first half of the project, the primary desired action is for members of the target audience to engage with the project, to help validate and optimise project activities and findings.

During the second half of the project, the primary desired action is for members of the target audience to:

- engage with the growing set of research findings
- engage as prospects for validations, refinement and adoption of commercial project outcomes.

3.2 Communications approach

3.2.1 Communications channels

From January 2017 (M3), the C3iSP project has supported these communication platforms

- Web site http://c3isp.eu/
- Social media (Twitter @C3ISP, LinkedIn)

The network provides an informal communication channel generally, and invited members of the network who attend a workshop offer a targeted and bi-direction communications around channel in a specific topic area.

The project will also liaise with local and international authorities (such as CERTs) to seek detailed domain information, and with other EU project to explore mutual benefit from their respective activities and outcomes.

3.2.2 Brand identity: logo, templates, etc.

By M3 the project will establish a standard set of branding, including logo, and document templates that unify and reinforce the branding.

3.2.3 Web portal

The web portal will be the primary source of dissemination of our project, as it will be the main contact for other researchers in the area. The C3ISP web portal will have different sections. In the main page, we will include the description of the project and will keep an update of the main news related to our project, including events. We also plan to maintain a section for the WPs where their work and main achievements can be described. A record of the publications we achieved will also be kept in the web page.

A responsive design will be selected, assuring easy reading and navigation on multiple devices: smart phones, tablets, notebooks and desktop PCs. The home page will be the project landing page and will contain the most important and up to date information in an easy to read format.

The C3ISP website will be designed operated by CNR. It will become operational in month 6 of the project, and will be continuously updated to facilitate better dissemination, outreach and project operation.

3.2.4 Social media

DigiCat will create a project landing page for promoting the C3IPS project and monitor the number of views. Furthermore, the Catapult will regularly promote project activity through LinkedIn and Twitter posts reaching an audience of 2000+ followers/contacts.

The Twitter handle @C3ISP will be created. All partners will be asked to contribute relevant content that can be shared.

The proposed approach for project promotion via Linkedin is to utilise the partner's exisiting accounts to achieve the desired traction and results. DigiCat will supply suggested posts for each of the partner to share with their own network.

Operationally this would follow the two steps below:

- Content (either blog/paper/event) is generated by partners and supplied to DigiCat
- DigiCat will create a post and share this with each partner to push out via their own Linkedin account, (ensuring consistent messaging).

3.2.5 Campaigns

There will be a marketing campaign aligned with each of these activities:

- Recruiting the Exploitation Board
- Notifying established networks of C3ISP activities – phase 1 & 2
- Recruiting attendees for each workshop.

3.2.6 Key messages

Communications from the project will be in the context of a unified set of key messages, which evolve as the project and its findings become refined.

During the initial phase of the project, the key messages echo the project mission statement that appears in Section (1.1).

Communications associated with the exploitation board will echo the terms of the Exploitation Board Agreement that is listed in Section (0).

Communications associated with research publications will summarise the abstract of the associated paper, poster or presentation.

During the second half of the project, messages for industrial stakeholders will reflect the business scenarios, and later the business cases.

In the last quarter of the project, messages will summarise project findings and achievements.

Table 5 shows the initial set of C3ISP messages, mapped to principle stakeholders.

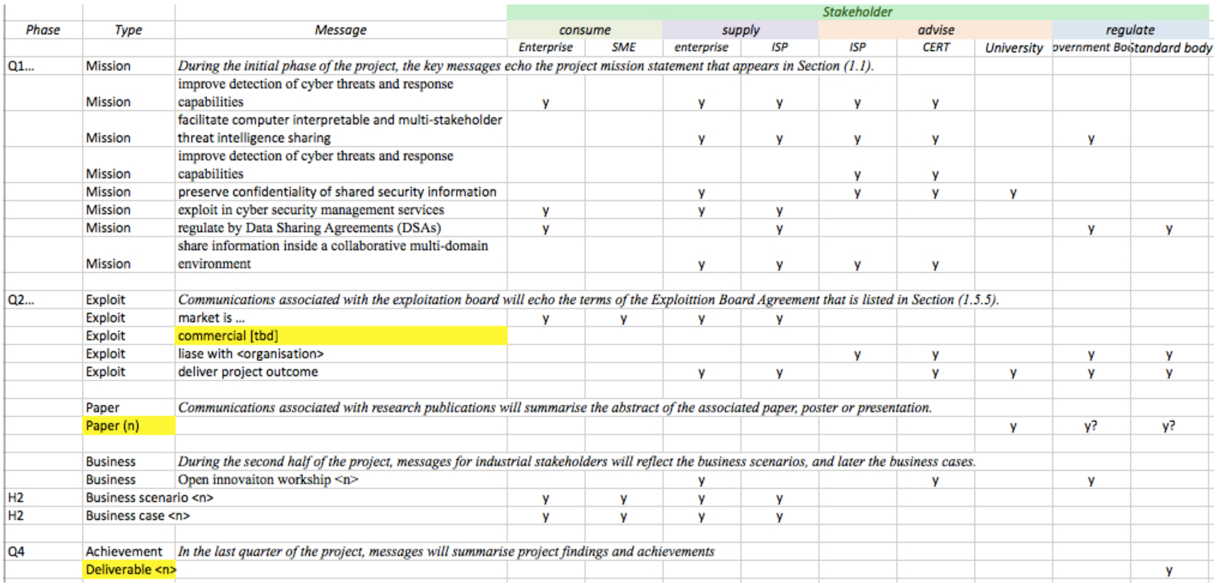
Each set of messages applies to a *Phase* of the project. Messages are classified by *Type*

which characterises its primary objective.

Stakeholders are grouped by the primary high-level class of influence (or call to action) that the communication associated with message seeks to have, including:

- Encourage the stakeholder to *consume* a C3ISP outcome
- Encourage the stakeholder to *supply* capability or information to support C3ISP outcomes, for example threat information
- *Advise* a stakeholder of C3ISP outcomes that are potentially important to them
- Influence bodies to change how they *regulate* security-related matters.

Table 5 - Initial C3ISP messages by stakeholder



			Stakeholder								
Phase	Type	Message	consume		supply		advise			regulate	
			Enterprise	SME	enterprise	ISP	ISP	CERT	University	overnment Bo	Standard body
Q1...	Mission	*During the initial phase of the project, the key messages echo the project mission statement that appears in Section (1.1).*									
	Mission	improve detection of cyber threats and response capabilities	y		y	y	y	y			
	Mission	facilitate computer interpretable and multi-stakeholder threat intelligence sharing			y	y	y	y		y	
	Mission	improve detection of cyber threats and response capabilities					y	y			
	Mission	preserve confidentiality of shared security information			y		y	y	y		
	Mission	exploit in cyber security management services	y		y	y					
	Mission	regulate by Data Sharing Agreements (DSAs)	y			y				y	y
	Mission	share information inside a collaborative multi-domain environment			y	y	y	y			
Q2...	Exploit	*Communications associated with the exploitation board will echo the terms of the Exploittion Board Agreement that is listed in Section (1.5.5).*									
	Exploit	market is ...	y	y	y	y					
	Exploit	commercial [tbd]									
	Exploit	liase with <organisation>					y	y		y	y
	Exploit	deliver project outcome			y	y		y	y	y	y
	Paper	*Communications associated with research publications will summarise the abstract of the associated paper, poster or presentation.*									
	Paper (n)								y	y?	y?
	Business	*During the second half of the project, messages for industrial stakeholders will reflect the business scenarios, and later the business cases.*									
	Business	Open innovaiton workship <n>			y			y		y	
H2	Business scenario <n>		y	y	y	y					
H2	Business case <n>		y	y	y	y					
Q4	Achievement	*In the last quarter of the project, messages will summarise project findings and achievements*									
	Deliverable <n>										y

3.3 Publications

3.3.1 Press release

Partners may handle their individual press releases independently, using agreed text.

In 2017, 3D Repo will be exhibiting the latest developments and results of this project during the Digital Construction Week trade show and also during the fourth British Information Modelling event where there will be a special session on cyber security and its implications on large-scale infrastructure projects across Europe.

These efforts are designed to pave the way for commercial exploitation that suits the relevant project partners in line with the current and future industrial environment in the EU where large amounts of sensitive data are being handled on daily basis.

3.3.2 Promotion

Project specific information will be created and distributed at relevant industry events, conference and workshops. Interactive public and project only forums will be created to support communication among the project participants and stakeholders.

We will make use of different media for the dissemination, including news articles, scientific journals, Internet, conferences, and workshops.

3.3.3 Brochure

A brochure will be created to support all partners in the promotion of C3ISP. This brochure will contain information on the C3ISP project objectives, information about the Consortium and the C3ISP approach to threat intelligence.

3.3.4 Videos

Footage of project meetings, capturing partner's contributions, debates and interviews will be recorded and shared via the appropriate media. 3DRepo will support the creation of these videos.

BT and SAP will produce a video of the joint demonstration they gave at the week-long BT Innovation 2017 event held at BT Adastral Park, Ipswich in June 2017. This demonstration was developed as part of C3ISP WP4 (Enterprise Pilot) and shows the application of differential privacy techniques to enable the analysis of pooled security data while safeguarding the security and confidentiality concerns of organisations contributing the data.

Digital Catapult will capture footage of their planned exploitation workshop(s), this will be produced in conjunction with other supporting documentation such as blogs and interviews.

3.3.5 Research papers

The project members plan more than fifteen publications that will be submitted, accepted and presented at peer-reviewed international conferences, and which acknowledge the C3ISP project. D9.2 contains a list of those already submitted. D9.3 will contain an updated list and D9.4 will contain the complete list at the end of the project.

3.3.6 Customised presentations

A standard presentation will be created to support all Partners in the promotion of C3ISP.

This presentation will contain information on the C3ISP project objectives, information about the Consortium and the C3ISP approach to threat intelligence, and be updated as the project progresses to summarise the growing set of outcomes.

A Consortium Partner may include slides from this presentation in their own slide-sets, and customise it to their needs, provided that:

- The essential messages are not materially changed
- The C3ISP project branding is retained, and C3ISP copyrights are respected.

3.4 Event schedule

3.4.1 Market Sector/Business Models – ‘Understand’ workshop [mid-project]

In consultation with the whole consortium we will identify which market sectors/business scenarios present the biggest need and commercial opportunity for further development of the C3ISP protection framework.

3.4.2 Market Sector/Business Models – ‘Validate & Prioritise’ workshop [mid-late project]

The aim of this workshop is to validate those market sectors and business scenarios identified during the ‘understand’ phase, with a specially selected target audience to ensure the propositions meet the needs of the market.

3.4.3 Exploitation Board – ‘Engage’ workshop [last quarter of the project]

The aim of this final workshop is to involve potential framework users and their ecosystems, along with members of the Exploitation Board to refine findings and raise awareness about the framework benefits and identify opportunities for commercial exploitation.

3.4.4 PhD school

CNR researchers will utilise significant experience of running summer schools (one of the oldest PhD summer schools in computer security) and organize the PhD school of C3ISP jointly with the one of NeCS. This is likely to be held in early 2018 in Trento, exact location to be confirmed.

The European Network for Cyber Security (NeCS, http://www.necs-project.eu/) is a Horizon 2020-funded cyber-security research and training network. It addresses the training and development of a European talent pool to help implement and support the European Cyber-security strategy as highlighted in the EC's Digital Agenda.

3.4.5 Conferences, seminars and industry events

Table 6 - Draft schedule of Conferences, seminars and industry events

Date	Type	Title	Location
June 2017	conference	Innovation 2017	BT R&D HQ, UK

3.5 Events participation & organisation

The template for reporting a partner's participation in an event is:

<event >[<partner>]

<event summary>

3.5.1.1 Description

3.5.1.2 Agenda

4 References

[1] Schawel, C., & Billing, F. (2014). Morphologischer Kasten. In C. Schawel & F. Billing, Top 100 Management Tools (1st ed.). Gabler Verlag

[2] Swemorph.com. Swedish Morphological Society. Retrieved 17 August 2017, from http://www.swemorph.com/index.html

[3] Wikipedia. SCAMPER. Retrieved 17 August 2017, from https://en.wikipedia.org/wiki/S.C.A.M.P.E.R

[4] Osterwalder, A. & Pigneur, Y. (2010) Business Model Generation.

[5] CSSA. Retrieved 17 August 2017, from https://www.cssa.de/en/index.html

[6] SAP. SAP Enterprise Threat Detection. Retrieved 17 August 2017, from https://help.sap.com/viewer/p/SAP_ENTERPRISE_THREAT_DETECTION

[7] 3D Repo. 3D Repo in a Secure Cloud Environment; a Case study, Retrieved 17 August 2017, http://3drepo.org/projects/3d-repo-in-a-secure-cloud-environment-a-case-study/

[8] ENISA. (2014). Standards and tools for exchange and processing of actionable information, November 2014. Retrieved 17 August 2017, https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information/at_download/fullReport

[9] IDEA. Intrusion Detection Extensible Alert. Retrieved 17 August 2017, from https://idea.cesnet.cz/en/index

[10] Data Harmonization Ontology. Retrieved 17 August 2017, from https://github.com/abusesa/abusehelper/blob/master/docs/Harmonization.md

Appendix 1. Glossary

Table 7 - Glossary

Acronym	Definition
AaaS	Application as a Service
BIM	Building Information Management
CERT	Community Emergency Response Team
CSSA	Cyber Security Sharing and Analytics
DDoS	Distributed Denial of Service
DSA	Data Sharing Agreement
ETD	Enterprise Threat Detection
GIS	Geographiuc Informationo System
IaaS	Infrastructure as a Service
IP	Intellectual Property
ISP	Internet Service Provider
MSS	Managed Security Service
OEM	Other Equipment Manufacturer
PTC	Patent Cooperation Treaty
SME	Small and Medium Enterprise
SVN	Apache Subversion
TI	Threat Intelligence