



D2.1 Cybersecurity and Privacy ecosystem model report - A Taxonomy of Cybersecurity and Privacy to assess the coverage of developed landscape by EC and nationally funded projects

| | |
|-----------|--------------------------------------|
| Author(s) | David Wallom & Michel Drescher, UOXF |
| Status | Final |
| Version | Final |
| Date | 12/04/2018 |

Dissemination Level

- PU: Public
 PP: Restricted to other programme participants (including the Commission)
 RE: Restricted to a group specified by the consortium (including the Commission)
 CO: Confidential, only for members of the consortium (including the Commission)

Abstract:

This deliverable acts as the first in a series of publications over the duration of the Cyberwatching.eu project detailing the process and methodology of quickly mapping and clustering European and national projects in a resilient cybersecurity framework.



The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

| | |
|---|---|
| Document identifier: Cyberwatching.eu – WP2 – D2.1 | |
| Deliverable lead | UOXF |
| Related work package | WP2 |
| Author(s) | D. Wallom & M. Drescher, UOXF |
| Contributor(s) | - |
| Due date | 31/04/2018 |
| Actual submission date | 12/04/2018 |
| Reviewed by | Nicholas Ferguson, Trust-IT; Mark Miller CPT; Alejandro Varas Gálvez, CITIC |
| Start date of Project | 01/05/2017 |
| Duration | 48 months |

Revision history

| Version | Date | Authors | Notes |
|---------|-----------|---|--|
| 0 | 5/2/2018 | David Wallom, Michel Drescher, UOXF | Initial content collection |
| 1 | 6/2/2018 | Michel Drescher, UOXF | Apply project document template |
| 2 | 3/4/2018 | David Wallom, Michel Drescher, UOXF | Update cross references, expand text, add EC projects in Annex A |
| 2.2 | 5/4/2018 | Nicholas Ferguson, Trust-IT; Mark Miller, CPT; David Wallom, UOXF | Changes based on feedback from internal review |
| 2.3 | 12/4/2018 | Alejandro Galvez, CITIC; Michel Drescher, UOXF | Changes from PMB review |
| Final | 12/4/2018 | Michel Drescher, UOXF | Final version |

Executive Summary

Ask a hundred people about cybersecurity, and you will get at least a hundred different opinions about what it actually means. Nonetheless, across all these different opinions one can identify a common theme or concern that are addressed.

One of the objectives of the Cyberwatching.eu project is to support projects in the cybersecurity domain in classifying and clustering themselves and others into meaningful groups of common topics and concerns to generate synergies and collaboration.

The process by which this is achieved involves a two-tier taxonomy of cybersecurity topics, against which European projects, both national and international, are first mapped against the first tier of domains of cybersecurity. Since many projects concern themselves with not only one domain, the three domains in the first tier are ranked according to the level of concern in the mapped project: High, medium, low, or not applicable: As a consequence, some projects are entirely out of scope, as the only concern themselves with *using* cybersecurity procedures or technology instead of *addressing* any of them as a concern of its own right.

This prioritised ranking allows the Cyberwatching.eu project to quickly and efficiently bring projects together and facilitate communication and synergies among them, so that the combined outputs will be larger than the mere sum of individual results.

This deliverable is the first in a series of reports addressing this objective of the Cyberwatching.eu project.

Section 1 provides the reader with an introduction into the larger topic and problem space and positions the Cyberwatching.eu project within the cybersecurity research landscape.

Section 2 introduces the reader to the mapping and clustering methodology used in this project.

Section 3 describes the Cyberwatching.eu cybersecurity research taxonomy that underpins the project's mapping and clustering efforts.

Section 4 positions the taxonomy in the wider research landscape, and compares it with other initiatives in this space, such as the NIST Critical Infrastructure Cybersecurity Framework, and the EC Survey Taxonomy. It also introduces a mapping between these three taxonomies.

Section 5 gives a complete account on the mapping and clustering methodology that is used in the Cybersecurity project in order to produce scientifically reproducible and resilient results.

In support to the previous section, Section 6 describes how the Cyberwatching.eu project identified and selected projects it admitted to the pool of mapped European cybersecurity projects.

The deliverable ends with section 7 detailing our next steps over the course of the project, and with section 8 providing conclusions on the results already achieved at this point.

Annexes A and B provide a complete list of all EU projects mapped so far, and the presentation given at the meeting with the EC JRC on comparing taxonomies, respectively.

Table of Contents

| | | |
|---|---|-----------|
| 1 | Introduction | 5 |
| 2 | Mapping and Clustering in Cyberwatching.eu | 7 |
| 3 | A cybersecurity taxonomy | 8 |
| 4 | Comparisons with Other Taxonomies | 11 |
| 4.1 | NIST Critical Infrastructure Cybersecurity Framework (CICF) | 11 |
| 4.2 | EC Survey Taxonomy | 13 |
| 5 | Clustering Methodology | 15 |
| 6 | Identification and mapping of relevant projects | 17 |
| 6.1 | Mapping EC projects to Cyberwatching.eu taxonomy categories | 17 |
| 7 | Next steps | 19 |
| 8 | Conclusion | 19 |
| Annex A. EC projects Mapped against the Taxonomy | | 20 |
| Annex B. Presentation given to Joint meeting on taxonomy alignment | | 25 |

Table of Figures

| | | |
|----------|--|----|
| Figure 1 | The interaction between workpackages within the Cyberwatching.eu project | 7 |
| Figure 2 | Output from clustering feeding into Cyberwatching.eu activities and hence into outputs consumed by key stakeholders..... | 7 |
| Figure 3 | Cybersecurity taxonomy as per cyber security architecture | 10 |
| Figure 4 | Matrix mapping of Cyberwatching.eu taxonomy to NIST CICF..... | 13 |
| Figure 5 | Mapping the Cyberwatching.eu clusters to the EC cybersecurity taxonomy categories | 14 |

Table of Tables

| | | |
|---------|--|----|
| Table 1 | Hierarchical arrangement of taxonomy categories and clusters | 10 |
| Table 2 | NIST CICF Functions and Categories; colour-coded by Cyberwatching.eu cluster mapping | 12 |
| Table 3 | Mapping NIST CICF categories to Cyberwatching.eu clusters | 12 |
| Table 4 | Mapping the Cyberwatching.eu taxonomy to the EC survey categories | 14 |

1 Introduction

Cybersecurity is a catch all description that is used in many spaces to describe a wide variety of different R&I activities, from the development of theoretical models for cryptography to the management of human computer interactions to ensure privacy is maintained. There are a very wide range of different definitions at the highest level available¹²³⁴⁵. Alongside these multiple high-level definitions, a number of different frameworks have been developed. These though consider for the most part (NIST, ECSSO etc.) how the different actions or activities to respond to a cybersecurity penetration or failure are managed. We feel that this is too deep a consideration and therefore it is still unclear how an R&I project that exists within the cybersecurity space may best reach out to other similarly targeted activities and know that they are going to have a realistic chance of alignment with key ongoing activities that make up the core of the two communicating activities. To give an indication of the scale of the activities in the cybersecurity space, the EC has allocated €600m to projects within this area, whilst the UK government on their own have supported activities worth £2bn. There are, as would be expected, a significant number of projects, both national and international. There is therefore the significant chance of overlap in activities, at best to allowed for shared learnings and at worst to support completely unnecessary duplication of activities.

Alongside the ability to more easily inform projects themselves about the possibilities of technical alignment with other relevant projects we also aim to support funding bodies themselves so they are able to understand the distribution of projects supported across the overall landscape and to identify imbalances which may mean over coverage of a certain area within the domain to the detriment of other parts. An overarching goal of Cyberwatching.eu is accelerating the development and deployment of cyber security and privacy research results and increasing Europe's ability to design and deliver innovative Internet services. In this timeframe, research and innovation projects have spearheaded the development of novel architectures and technologies, which can protect our European Digital Society against cybersecurity threats. Cyberwatching.eu will address these and similar challenges through its observation of national and pan-European R&I initiatives, standards, policy and regulation, and market needs.

We will first define a taxonomy of cybersecurity, to allow a single uniform understanding of the different sub areas of cybersecurity R&I to be established. This will be a two-layer design, firstly a top-level set of three domains and then a subset of 6 areas which are individually indivisible. Once these definitions are described we then rank the importance of initially each top-level domain and then each area for every project for which we have information. These rankings are then turned into numerical scores and a statistical analysis performed against them. The output being a quantitative analysis of the project based on their relevance to the domains and areas. To validate the scoring, we will communicate with the projects discussing the scorings that have been given to them by the CW team and discuss specifically the results for

¹ <https://www.enisa.europa.eu/publications/definition-of-cybersecurity>

² <https://en.oxforddictionaries.com/definition/cybersecurity>

³ <http://niccs.us-cert.gov/glossary/#cybersecurity>

⁴ <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>

⁵ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

their own projects that we have identified. As national projects have little or no reason to be early engagers/adopters the projects chosen for this will be those supported by the EC, where if necessary pressure from the funder to engage can be used. This statistical method of project alignment and analysis has been previously used within the Cloudwatch and Cloudwatch2 projects to successfully analyse the Cloud computing landscape using and then validating the NIST model of cloud computing⁶.

⁶ Caithness, N., Drescher, M. & Wallom, D. Can functional characteristics usefully define the cloud computing landscape and is the current reference model correct? J Cloud Comp (2017) 6: 10. <https://doi.org/10.1186/s13677-017-0084-1>

2 Mapping and Clustering in Cyberwatching.eu

Within the Cyberwatching.eu project the clustering of projects is a fundamental step in the value chain that the project provides overall. As can be seen in figure X the work of WP2 is the generator of information on projects at both a national and pan European scale that are available to work with the Cyberwatching.eu activity overall. The work package and hence activity feeds into both the Concertation activity, i.e. where we are aiming to bring together the community of projects in a manner which is beneficial to them and the EC so they better understand the landscape of cybersecurity and where they have placed projects within it.

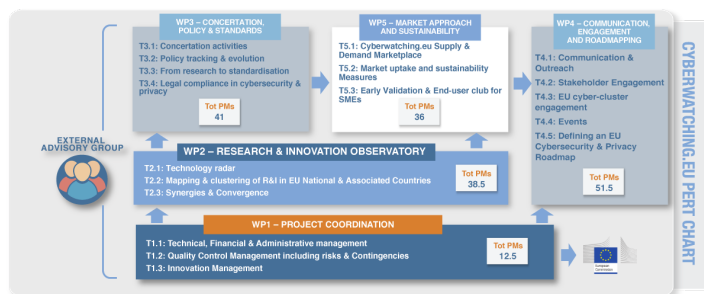


Figure 1 The interaction between workpackages within the Cyberwatching.eu project

The clustering is the first stage for two crucial activities within the Cyberwatching.eu project, as shown in figure 2. Here we describe the outputs which feed into the different stakeholder groups and the vehicles to ensure that those outputs are as relevant as possible.



Figure 2 Output from clustering feeding into Cyberwatching.eu activities and hence into outputs consumed by key stakeholders.

3 A cybersecurity taxonomy

The taxonomy as developed within Cyberwatching.eu is intended to allow the identification of different aspects of cybersecurity and from this the way that different projects and activities concentrate on different sub areas in their developments.

The two-layer design of the taxonomy is not a new concept; for example, the NIST Cybersecurity Framework definition⁷ being a functional taxonomy focusing on improving the outcomes of cybersecurity implementations uses three levels of refinement: Function – Category – Subcategory. It is therefore primarily targeting and useful in the *operational* domain of cybersecurity. The overlap in topics between the NIST definition and the Cyberwatching.eu taxonomy is of complementary rather competitive nature: The difference lies in the intended outcome and result of these works. For instance, while both the NIST definition and the Cyberwatching.eu taxonomy both include the issue of intra- and inter-organisational attack propagation and containment, NIST looks at it from an organisational IT management perspective:

- Identify – e.g. “Is there a risk, and can we quantify it?”
- Protect – e.g. “What protective technology do we use against it?”
- Detect – e.g. “What detection tools and processes are implemented?”
- Respond – e.g. “How do we mitigate, and communicate?”
- Recover – e.g. “What systems were affected, when and how to we improve them?”

In contrast, the Cyberwatching.eu taxonomy looks at it from the research and innovation perspective, looking to improve the body of knowledge as well as increase the variety and depth of the toolbox available to deploy and exploit: Staying in the example of attack propagation; the Cyberwatching.eu cluster “Human aspects of cybersecurity” includes human interaction with digital systems, system usability (or the lack thereof) or cultural diversity: All these aspects are important, and apply to different functional NIST categories: Interaction with digital systems may inform how attack propagation occurs within and across organisations (e.g. distributing malware-infected images or videos on current social media memes) as well as how one might protect infrastructure against it. But cultural differences of how digital systems are used (e.g. Anglo-Saxon usage patterns vs. east Asian media usage patterns) may inform how to respond to the same threat in different cultural contexts, or even how to communicate (use of language, authoritarian vs. non-authoritarian cultures) attack propagation across organisation and geographic regions.

The high-level definitions created are;

- **Foundational technical methods & risk management for trustworthy systems in cybersecurity and privacy** – The development of technologies that are directly associated with cybersecurity capabilities or features and methods by which the confidence in the technical capabilities of a system may be validated.
- **Applications and user-oriented services to support cybersecurity and privacy** – Specific capabilities or services which directly interact with system users and are developed with capabilities that are directly about how to improve the inherent capabilities and user experiences of cybersecurity and privacy in consumed services.
- **Policy, governance, ethics, trust, and usability, human aspects of cybersecurity & privacy** – Aspects of cyber security that are overwhelmingly driven by the human interaction, understanding and dependency on how secure systems are or have been designed to be.

⁷ <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

Sitting below these top-level domains are, as discussed, further subdivisions which look at the main areas, which then cover what we would consider the whole landscape. Within the consortium the following subdivision is optimal;

- **Secure systems and technology:** How security can be built into technology from the design stage including cloud computing security, cryptography, trusted platforms, wireless security, mobile security and secure coding paradigms.
- **Verification and assurance:** Two disciplines that help establish how much confidence you can have in a system, both in terms of security and the privacy of all stakeholder groups who act with or in a system. Assurance focuses on managing risks related to the use, processing, storage, and transmission of information, whereas formal verification seeks to build a mathematical model of a digital system and then try to prove whether it is 'correct', often helping to find subtle flaws.
- **Operational risk, management and analytics:** Understanding the risk and harm resulting from cyberattacks, and how it propagates across and between organisations. Work focuses on creating situational awareness through aiming for a complete understanding of scenario and risk management; metrics and models for security postures; and analytics for predicting risk, prioritising responses and supporting security operations.
- **Identity, behaviour, ethics and Privacy:** Bringing diverse perspectives and interpretations to questions such as: Who are you online, how do you communicate, and what can (or should) you do? This also connects to the ongoing activities on Privacy launched through directives and regulations over the past year.
- **National and international security, privacy and governance:** looking at politics, international relations, defence, policy and governance issues: how do countries and communities interact with (and through) technology, and how might this change in different contexts?
- **Human aspects of cyber security:** Understanding the ways humans interact with (and through) digital systems – whether to understand and design for target users, or to understand how adversaries operate and can exploit the systems. This includes aspects like usability, trust, collaborative practices, social embeddedness, nationhood, cultural diversity, impact on economy, and the relationship between microsocial interactions and global structures.

This two-tier taxonomy allows for a number of meaningful arrangements. The most obvious arrangement is a hierarchical model, which is the default for this taxonomy (see Table 1).

| Level 1: Category | Level 2: Cluster |
|---|--|
| Foundational technical methods & risk management for trustworthy systems in cybersecurity & privacy | Operational Risk and Analytics |
| | Verification and Assurance |
| Applications and user-oriented services to support cybersecurity and privacy | Secure Systems and Technology |
| | Identity, Behaviour, Ethics and Privacy |
| Policy, governance, ethics, trust, and usability, human aspects of cybersecurity & privacy | National and international security and governance |
| | Human Aspects of Cybersecurity |

Table 1 - Hierarchical arrangement of taxonomy categories and clusters

A hierarchical arrangement allows for quick and efficient mapping of projects into categories, effectively facilitating projects to form groups of meaningful size and "gravity" to instigate conversations and discovering overlaps and synergies.

The implicit rule of hierarchical grouping does not allow "jumping" the cluster when further differentiating the projects into cluster: A change of category indicates one of two conditions:

- The initial categorisation was incorrect, or
- The hierarchical arrangement of the taxonomy is insufficient.

Both conditions can be detected early on as soon as differentiating projects into clusters will begin – they hence form built-in auto-correction features of the taxonomy.

The other suitable arrangement refers to an understanding of cybersecurity architecture as follows.

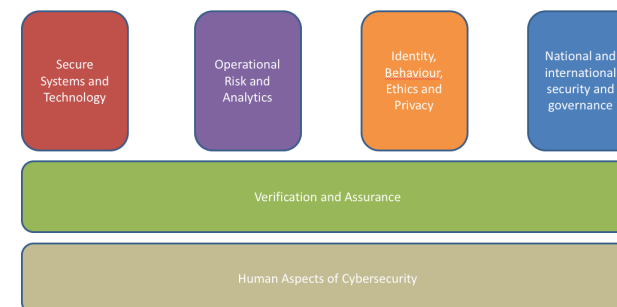


Figure 3 - Cybersecurity taxonomy as per cyber security architecture

The taxonomy's architectural arrangement illustrated in Figure 3 highlights the need of cross-cluster communication facilitation despite clustering along the hierarchy of the taxonomy: Despite being allocated to specific categories, *Verification and Assurance*, and *Human aspects of Cybersecurity* are cross-cutting issues in the cybersecurity landscape, and therefore need to be treated accordingly.

4 Comparisons with Other Taxonomies

It was decided that since there are a number of different taxonomies available that it would be relevant and useful to compare the Cyberwatching.eu taxonomy with two other leading activities in this area. Therefore, the NIST Critical Infrastructure Cybersecurity Framework (CICF) and the EC Cybersecurity Competency Survey Taxonomy were chosen for comparison. In each of these cases we have made both single and multi-dimensional comparisons. This was done as though a one-to-one mapping of terms, definitions and areas is desirable, it is highly likely that there will be multiple areas where there is alignment so a matrix of comparison in both cases had been produced.

4.1 NIST Critical Infrastructure Cybersecurity Framework (CICF)

The NIST CICF⁸ defines five top level functions and within each of these up to 6 categories. Since the framework has a different overall target we have considered how the categories map to the Cyberwatching.eu categories and clusters. This first single allocation is given in Table 2 below in the NIST ordering format, with colour-coding to indicate which Cyberwatching.eu cluster each NIST category has been mapped to.

| NIST CICF Function | NIST CICF Category |
|--------------------|---|
| Identify | Asset Management |
| | Business Environment |
| | Governance |
| | Risk Assessment |
| | Risk Management Strategy |
| Protect | Access Control |
| | Awareness and Training |
| | Data Security |
| | Information Protection Processes and Procedures |
| | Maintenance |
| | Protective Technology |
| Detect | Anomalies and Events |
| | Security Continuous Monitoring |
| | Detection Processes |
| Respond | Response Planning |
| | Communications |
| | Analysis |
| | Mitigation |

⁸ <https://www.nist.gov/sites/default/files/documents///draft-cybersecurity-framework-v1.11.pdf>

| NIST CICF Function | NIST CICF Category |
|--------------------|--------------------|
| Recover | Improvements |
| | Recovery Planning |
| | Communication |

Table 2 - NIST CICF Functions and Categories; colour-coded by Cyberwatching.eu cluster mapping

The following table rearranges this mapping to order NIST categories to Cyberwatching.eu taxonomy clusters:

| Cyberwatching.eu cluster | NIST CICF Category (Function) |
|---|---|
| Secure systems and technology | Data security (Protect) |
| | Maintenance (Protect) |
| | Protective Technology (Protect) |
| | Anomalies and Events (Detect) |
| | Security Continuous Monitoring (Detect) |
| Verification and Assurance | Risk Management Strategy (Identify) |
| | Detection Processes (Detect) |
| | Analysis (Respond) |
| Operational risk, management and analytics | Asset Management (Identify) |
| | Risk Assessment (Identify) |
| | Response Planning (Respond) |
| | Recovery Planning (Recover) |
| Identity, behaviour, ethics and Privacy | Access Control (Protect) |
| | Mitigation (Respond) |
| | Improvements (Recover) |
| National and international security and governance | Business Environment (Identify) |
| | Governance (Identify) |
| | Information Protection Processes and Procedures (Protect) |
| Human aspects of cyber security | Awareness and Training (Protect) |
| | Communications (Respond) |
| | Communications (Recover) |

Table 3 - Mapping NIST CICF categories to Cyberwatching clusters

As can be seen, there are a number of instances within this one to one matchings that would be comfortable with another allocation to domain area. Therefore, we then consider the matrix matching between the two taxonomies.

As we assume that due to the differing goals of both the Cyberwatching.eu and NIST taxonomies there are likely to be multiple areas of overlap, we have created the following matrix comparison between the two.

| | | NIST | | | | | | | | |
|---------------|--|--|---------|--------|---------|---------|--|--|--|--|
| | | Identify | Protect | Detect | Respond | Recover | | | | |
| Cyberwatching | Technology & Risks | Operational Risk and Analytics | | | | | | | | |
| | Apps & user oriented services | Secure Systems and Technology | | | | | | | | |
| | Policy & Governance | National & int'l security and governance | | | | | | | | |
| | | Human Aspects of Cybersecurity | | | | | | | | |
| | | | | | | | | | | |

Figure 4 - Matrix mapping of Cyberwatching.eu taxonomy to NIST CICF

4.2 EC Survey Taxonomy

As part of efforts by the EC to understand the Cybersecurity landscape⁹, the EC has commissioned a study through the EC JRC for which a specific taxonomy has been developed. We have compared terms as below, as these are top level domains in themselves we have ordered them as per the Cyberwatching.eu taxonomy for ease of understanding overlaps.

| Cyberwatching.eu Clusters | EC Survey Categories |
|---|---|
| Secure systems and technology | Cryptology |
| | Network and Distributed Systems |
| | Software and Hardware Security Engineering |
| Verification and Assurance | Assurance, Audit and Certification |
| | Theoretical Foundations of Security Analysis and Design |
| Operational risk, management and analytics | Operational Incident Handling and Digital Forensics |
| | Security Measurements |
| | Identity and Access Management (IAM) |

⁹ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017>

| Cyberwatching.eu Clusters | EC Survey Categories |
|---|---|
| Identity, behaviour, ethics and Privacy | Technology and Legal Aspects |
| | Trust Management, Assurance, and Accountability |
| National and international security and governance | Data Security and Privacy |
| | Security Management and Governance |
| Human aspects of cyber security | Human Aspects |
| | Education and Training |

Table 4 - Mapping the Cyberwatching.eu taxonomy to the EC survey categories

The following matrix visualization illustrates the mapping in a similar fashion to the mapping of the NIST CICF functions and categories:

| | | EC Taxonomy categories | | | | | | | | | | | | | |
|---------------|--|--|------------|---------------------------|------------------------|---|---------------|--------------------------------------|------------------------------------|---------------------------------|--|-----------------------|------------------------------|---|---|
| | | Assurance, Audit and Certification | Cryptology | Data Security and Privacy | Education and Training | Operational Incident Handling and Digital Forensics | Human Aspects | Identity and Access Management (IAM) | Security Management and Governance | Network and Distributed Systems | Software and Hardware Security Engineering | Security Measurements | Technology and Legal Aspects | Theoretical Foundations of Security Analysis and Design | Trust Management, Assurance, and Accountability |
| Cyberwatching | Technology & Risks | Operational Risk and Analytics | | | | | | | | | | | | | |
| | Apps & user oriented services | Secure Systems and Technology | | | | | | | | | | | | | |
| | Policy & Governance | National & int'l security and governance | | | | | | | | | | | | | |
| | | Human Aspects of Cybersecurity | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |

Figure 5 - Mapping the Cyberwatching.eu clusters to the EC cybersecurity taxonomy categories

In addition to the previously discussed work on matching taxonomy areas we have organised a meeting with representatives of Cyberwatching.eu, ECSO WG6 and the authors of the EC JRC taxonomy. The Cyberwatching.eu project officer was also present and asked to describe the EC expectations from cyberwatching.eu & ECSO alignment on cybersecurity & privacy taxonomies.

Each group was asked to present their taxonomy, rationale for development and how they viewed alignment. The Cyberwatching.eu presentation given at the meeting is attached as Annex B and we were able to provide feedback to both other participating groups of how their and our work related, overlapped and was complementary.

5 Clustering Methodology

Cyberwatching.eu will provide a platform for fostering project collaboration, through a two-stage clustering of projects thereby allowing cross pollination of both non-technical policy, experience and best practice findings as well as deeper technical specifics bringing expertise from across the top-level cluster together to concentrate on specific issues coming together in smaller and more tightly focused groups. These will be taking an in-depth look at specific common topics, sharing updates with EC representatives and taking stock of progress. This also supports the promotion of research and innovation results and the meta layer grouping and lays the basis for further analysis of the ecosystem.

The first meta clustering is to bring together those projects whose overall externally described goals are aligned. This uses the high-level definitions previously discussed. The membership of these clusters will be defined by the high-level goals of projects as described by their public descriptions. This will allow a coming together of projects whose high levels goals may be more closely aligned rather than some attempts to create projects synergies that just attempt to bring together all projects that have been funded through a specific route or another.

Going beyond these top-level groupings we will then assess each of the projects within the communities to be supported to create a more quantifiably driven clustering around more technically focused capabilities or components within projects. This analysis of European cybersecurity and privacy projects will give a way also for the wider community and the EC to gain insight into where the projects are located within the cybersecurity and privacy landscape. The objective of this empirical analysis is to discover distinct smaller groups of projects that are consistent in their relationship to a set of defined general characteristics. These clusters of projects will form the basis for identifying:

- Future collaboration and sharing of experience on common technical priorities
- Re-use of project results by other current and future projects with components, technical ideas, methodologies or best practices identified by a repeatable statistical analysis rather than qualitative methodologies.
- Identify market positioning and potential exploitation opportunities with other projects

The higher-level identification of the criteria upon which the clustering is able to be done is based on a schema for the way that Cybersecurity and Privacy, methods, research and innovation may be classified in a number of different ways.

Cyberwatching.eu will start the analysis by collecting a dataset representing currently funded European projects and scored against the full set of identified defining characteristics on an interval scale. To support the data collection, an online tool will be delivered which analyses detailed knowledge of the cybersecurity landscape, and demonstrates how different projects form natural clusters based on their common relationship to a set of defining features.

The clustering procedure is based on the outcome of a classic Principal Components Analysis (PCA)¹⁰. We will visualise the landscape on a simultaneous biplot of the

¹⁰ (a) Pearson, K. 1901. On Lines and Planes of Closest Fit to Systems of Points in Space. *Philosophical Magazine*, 2 (11): 559–572. (b) Hotelling, H. 1933. Analysis of a complex of statistical variables into principal components. *Journal of Educational Psychology*, 24, 417–441, and 498–520. (c) Jolliffe, I.T. 2002. *Principal Component Analysis*, 2nd edition, Springer-Verlag.

characteristic coefficients and component scores¹¹. As a natural extension of the biplot we project scores from a reduced dimensionality PCA space onto the coefficient vectors and use those score for clustering. We will employ a classic Euclidian distance single linkage hierarchical clustering¹². This statistical approach has been shown to be successful within the Cloud Computing space in CloudWatch and CloudWatch2 by identifying activities who otherwise would have ignored each other as prospects for technical experience or product sharing but who have a significant technical aligned which would have otherwise been missed.

Based on the analysis results, Cyberwatching.eu will home in on a maximum of 4 priority areas and actively engage with clustered projects in a series of activities which incentivises and encourages projects to contribute. These include:

- 4 Technology deep dive workshops to map existing solutions to priority areas and enable common approaches to similar challenges and facilitate re-use of research results
- White-papers focussing on challenges to be addressed by future Work Programmes
- Test and validate market readiness of solutions

¹¹ (a) Gabriel, K.R. 1971. The biplot graphic display of matrices with application to principal component analysis. *Biometrika*, 58 (3): 453–467. (b) Gabriel, K.R. 1981. Biplot display of multivariate matrices for inspection of data and diagnosis. In V. Barnett (Ed.) *Interpreting multivariate data*. London, John Wiley & Sons. (c) Greenacre, M. 2010. *Biplots in Practice*. BBVA Foundation, Madrid, Spain.

¹² (a) Hastie, T., Tibshirani, R. and Friedman, J. 2009. *Hierarchical clustering*. In *The Elements of Statistical Learning*, 2nd edition, New York, Springer. pp. 520–528. (b) The Mathworks ® R2015a Documentation. Agglomerative hierarchical cluster tree.

6 Identification and mapping of relevant projects

The identification of relevant projects to include within the clustering exercise is key. As part of this a methodology was chosen whereby different consortium partners were asked to collect and contribute references and public contact details of cybersecurity projects.

First, all project partners were asked to summarise as to which EU member countries their cybersecurity professional network would extend. This information was captured in a confidential tabulation.

Next, all 28 Member states were allocated to Cyberwatching.eu project partners to gather *public* information about publicly funded cybersecurity projects in the member states. The allocation was done following two guidelines:

- The candidate country MUST be part of the respective partner's network, and
- The candidate country SHOULD be neighbouring, or as close as possible, to already allocated countries.

In parallel, the project's overall network power, ties to the Commission through the project's appointed EC project officer, and the use of the publicly available CORDIS system¹³ a large number of past and present EC-funded cybersecurity projects were collected and added to the source material.

This source list is maintained as a living list, i.e. projects are added as and when they become known to us.

At the time of writing, this list includes:

- 147 EC funded projects
- 7 Italian projects
- 13 French projects
- 3 Albanian project sources (i.e. sources which collect project information)
- 3 Lithuanian project sources
- 2 Slovenian projects
- 7 German project sources
- 13 other cybersecurity initiatives

Our initial plan was confirmed by the expected results of data gathering: A vast majority of European projects, and in comparison, rather few national projects. Though this has in some ways been hindered by the lack of clear methods by which we are able to access lists, details or contact points for national projects. Our initial plan to map European projects first as a quick start of activities followed by more resource-intensive research of national projects (expected to be hindered by language barriers) was thus proved to be a good strategy, and put into motion. We are aiming to utilize contacts within Cyberwatching.eu who are part of ECSO as gateways to access countries for which we currently have no information. It is therefore we consider not at this point suitable to add KPI around numbers of national projects per country that we are able to contact though when we have at least the contact details of a competent national authority who may have national level information this may change.

6.1 Mapping EC projects to Cyberwatching.eu taxonomy categories

Initially we are using the three Level 1 categories as described in section 3:

- Foundational technical methods & risk management for trustworthy systems in cybersecurity and privacy

¹³ https://cordis.europa.eu/projects/home_en.html

- Applications and user-oriented services to support cybersecurity and privacy
- Policy, governance, ethics, trust, and usability, human aspects of cyber security & privacy

Annex A lists all European projects that will be mapped in the first phase of the exercise.

Unlike in the Cloudwatch2 project, where projects were *scored* against the 13 NIST cloud computing characteristics, EC projects are being *ranked* against the Cyberwatching.eu taxonomy categories: The difference lies in the resulting score matrix: While scoring allows the same scoring value to be given for different characteristics (Cloudwatch2), ranking forces a decision as to which of the categories (Cyberwatching.eu) is most important, important, or least important for the given project. Translated into numerical scores, ranking will never see any two categories with the same score for any give project.

Also, Cyberwatching.eu allows for taxonomy categories to be *out of scope* and therefore not to be ranked for a given project. In fact, preliminary results indicate that there is indeed a small number of projects that cannot be ranked at all! In other words, they would not qualify as projects where cybersecurity would be a research of innovation topic.

In terms of statistical analysis, the process needs to cater for *definition holes* – equivalent to “no answer given” in surveys that allow answers to be skipped. In this context definition holes are a result of a taxonomy category being out of scope for a project.

While this may be counterintuitive at first, we expect the allowance of definition holes to result in significantly increased accuracy of the analysis of the initial mapping exercise as will be described in future deliverables.

7 Next steps

We will be presenting the preliminary analysis of the projects at the first Cyberwatching.eu Concertation meeting on the 26th April 2018. This will give the opportunity for the projects to provide input to both the definitions of the Level 1 categories but also see for themselves where they have currently been allocated. Following on from this we are aiming to start the scoring process for projects with the level 2 taxonomy such that clustering will provide validations through bootstrapping of the overall project scoring and allocation mechanism.

8 Conclusion

Within this deliverable, we have described the taxonomy that the Cyberwatching.eu project have developed to enable an analysis to be completed of national and European cybersecurity projects. This will construct both a map of the ecosystem as a whole but also facilitate the clustering of projects that are aligned under specific thematic areas within the ecosystem. It is aimed that this will have a number of benefits including effective concertation for EC supported projects and ensuring more widely that best practice may be more easily shared as those projects coming together are actually structurally and thematically aligned.

The taxonomy developed has two levels, the Level 1 categories and the Level 2 clustering themes. An unusual item within the taxonomy is the fact that not all of the Level 2 clustering items are unique. It is clear for example that the two areas of verification and Assurance and Human aspects are cross cutting themes and the analysis undertaken of results will have to take this into account. We will of course also be able to verify that these really are cross cutting through the hierarchical clattering process.

To validate the taxonomy, we have attempted to match our terms with those in other models, in this case one each from NIST and the EC. It was clear following analysis that we have covered all areas within these though the allocation of sub terms to our level 2 terms could be done in a number of different ways depending on the opinion of the author that is doing the allocation.

Following the identification of projects, both national and international we have within the team completed a first pass analysis of the allocation of projects to the Level 1 categories. Following this we will then complete this for the Level 2 categories as well. We will through the EC projects in the area request that the projects verify our scores for a small number of projects so that we are able to confirm the methodology. Once this has been done a full analysis will be completed.

Overall we believe that our taxonomy describes the full breadth of what could be the cybersecurity landscape and hence with analysis will be a useful tool to enable projects to understand not only the whole landscape but also their place within it.

ANNEX A. EC PROJECTS MAPPED AGAINST THE TAXONOMY

| Project | Call | Type | End | Project URL |
|---------------|-----------------|--------|----------|---|
| AARC2 | EINFRA-22-2016 | RIA | Apr 2019 | |
| ABC4Trust | ICT-2009.1.4 | CP | Feb 2015 | https://abc4trust.eu/ |
| ADDPRIV | SEC-2010.6.5-2 | CP | Mar 2014 | http://www.addpriv.eu/ |
| AEGIS | DS-05-2016 | CSA | Apr 2019 | http://aegis-project.org/ |
| ANASTACIA | DS-01-2016 | RIA | Dec 2019 | http://www.anastacia-h2020.eu/ |
| ARIES | FCT-09-2015 | RIA | Feb 2019 | http://aries-project.eu/ |
| ARMOUR | ICT-12-2015 | RIA | Jan 2018 | http://www.armour-project.eu/ |
| ASAP | ERC-AG-PE6 | ERC-AG | Sep 2018 | |
| ATENA | DS-03-2015 | IA | Apr 2019 | https://www.atena-h2020.eu |
| BEACON | ICT-07-2014 | RIA | Jul 2017 | http://www.beacon-project.eu/ |
| BIOSEC | FP7-PEOPLE | MC-IOF | Feb 2012 | |
| C3ISP | DS-04-2015 | IA | Sep 2019 | https://www.digitalcatapultcentre.org.uk/project/c3isp/ |
| CANVAS | DS-07-2015 | CSA | Aug 2019 | https://canvas-project.eu/canvas/ |
| certMILS | DS-01-2016 | IA | Dec 2020 | https://certmils.eu/ |
| CHOReVOLUTION | ICT-09-2014 | RIA | Dec 2017 | http://www.chorevolution.eu/bin/view/Main/# |
| CIPSEC | DS-03-2015 | IA | Apr 2019 | http://www.cipsec.eu |
| CITADEL | DS-03-2015 | IA | May 2019 | http://www.citadel-project.org |
| CLARUS | ICT-07-2014 | RIA | Dec 2017 | http://clarussecure.eu/ |
| CloudSocket | ICT-07-2014 | RIA | Dec 2017 | https://site.cloudsocket.eu/ |
| CloudTeams | ICT-07-2014 | IA | Feb 2017 | https://www.cloudteams.eu/projects/ |
| COCKPITCI | SEC-2011.2.5-1 | CP-FP | Dec 2014 | |
| COEMS | ICT-10-2016 | RIA | Oct 2019 | https://www.coems.eu/ |
| COLA | ICT-06-2016 | IA | Jun 2019 | http://www.project-cola.eu/ |
| COMPACT | DS-02-2016 | IA | Oct 2019 | |
| CONSENT | SSH-2009-3.2.1. | CP-FP | Apr 2013 | http://consent.law.muni.cz/ |
| CREDENTIAL | DS-02-2014 | IA | Sep 2018 | https://credential.eu/ |
| CROSSMINER | ICT-10-2016 | RIA | Dec 2019 | https://www.crossminer.org/ |
| CryptoCloud | ERC-AG-PE6 | ERC-AG | May 2019 | |
| CS-AWARE | DS-02-2016 | IA | Aug 2020 | |
| CYBECO | DS-04-2016 | RIA | Apr 2019 | https://www.cybeco.eu/ |
| CyberWiz | DRS-17-2014 | SME-2 | Aug 2017 | https://www.cyberwiz.eu/ |
| CYCLONE | ICT-07-2014 | IA | Dec 2017 | http://www.cyclone-project.eu/ |

| | | | | |
|-------------|------------------|--------|----------|---|
| CYRail | S2R-OC-IP2- | RIA | Sep 2018 | |
| DAPPER | FP7-PEOPLE | MC-CIG | Mar 2018 | |
| DECODE | ICT-12-2016 | RIA | Nov 2019 | https://www.decodeproject.eu |
| DEFENDER | CIP-01-2016-2017 | IA | Apr 2020 | |
| DISCOVERY | ICT-38-2015 | CSA | Dec 2017 | |
| DiSIEM | DS-04-2015 | IA | Aug 2019 | http://disiem-project.eu |
| DITAS | ICT-06-2016 | RIA | Dec 2019 | http://www.ditas-project.eu/ |
| DOGANA | DS-06-2014 | IA | Aug 2018 | http://www.dogana-project.eu |
| DSSC | MSCA | MSCA | Apr 2022 | |
| e-Sides | ICT-18-2016 | CSA | Dec 2019 | http://www.e-sides.eu/ |
| ECRYPT-CSA | ICT-32-2014 | CSA | Feb 2018 | http://www.ecrypt.eu.org/csa/ |
| ECRYPT-NET | MSCA- | MSCA | Feb 2019 | http://www.ecrypt.eu.org/net/ |
| ENCASE | MSCA-RISE | MSCA | Dec 2019 | http://encase.socialcomputing.eu/ |
| EU-SEC | DS-01-2016 | IA | Dec 2019 | http://www.sec-cert.eu/ |
| EUNITY | DS-05-2016 | CSA | May 2019 | |
| FIDELITY | SEC-2011.3.4-1 | CP-IP | Jan 2016 | http://www.fidelity-project.eu/ |
| FORTIKA | DS-02-2016 | IA | May 2020 | |
| FutureTrust | DS-05-2015 | IA | May 2019 | https://www.futuretrust.eu/home/ |
| GenoPri | MSCA | MSCA | Apr 2018 | |
| GHOST | DS-02-2016 | IA | Apr 2020 | http://www.ghost-project.eu |
| HEAT | ICT-32-2014 | RIA | 43100 | https://heat-project.eu/ |
| HECTOR | ICT-32-2014 | RIA | Feb 2018 | https://hector-project.eu/ |
| HERMENEUT | DS-04-2016 | RIA | Apr 2019 | https://cyberconnector.eu/web/hermeneut |
| HIPS | ERC-CG | ERC-CG | Sep 2019 | |
| IMPACT | ERC-2013-SyG | ERC | Jan 2021 | http://www.impact-erc.eu/ |
| KONFIDO | DS-03-2016 | RIA | Oct 2019 | http://www.konfido-project.eu/konfido/ |
| LAST | ERC-SG-PE6 | ERC-SG | Sep 2014 | |
| LIGHTest | DS-05-2015 | IA | Aug 2019 | http://lightest.eu |
| LV-Pri20 | MSCA-IF-2014 | MSCA | Jun 2017 | |
| MAMI | ICT-12-2015 | RIA | Jun 2018 | https://mami-project.eu/ |
| MAPPING | SiS.2013.1.2-1 | CSA-SA | Feb 2018 | https://mappingtheinternet.eu/ |
| MAS2TERING | ICT-2013.6.1 | CP | Aug 2017 | http://www.mas2tering.eu/ |
| MATTHEW | ICT-2013.1.5 | CP | Oct 2016 | https://matthew-project.eu/ |
| MELODIC | ICT-06-2016 | RIA | Nov 2019 | |

| | | | | |
|--------------------|------------------|--------|----------|---|
| mf2C | ICT-06-2016 | RIA | Dec 2019 | http://www.mf2c-project.eu/ |
| MH-MD | ICT-18-2016 | RIA | Oct 2019 | http://www.myhealthmydata.eu |
| MIKELANGELO | ICT-07-2014 | RIA | Dec 2017 | https://www.mikelangelo-project.eu/ |
| MITIGATE | DS-06-2014 | IA | Feb 2018 | http://www.mitigateproject.eu |
| MUSA | ICT-07-2014 | RIA | Dec 2017 | http://www.musa-project.eu/ |
| NECOMA | ICT-2013.10.1 | CP | Mar 2016 | http://www.necoma-project.eu/ |
| NeCS | MSCA | MSCA | Aug 2019 | http://www.necs-project.eu/ |
| OCGN | MSCA | MSCA | Nov 2018 | |
| OCTAVE | DS-02-2014 | IA | Jul 2017 | https://www.octave-project.eu/ |
| OPENREQ | ICT-10-2016 | RIA | Dec 2019 | http://openreq.eu/ |
| OPERANDO | DS-01-2014 | IA | Apr 2018 | http://www.operando.eu/ |
| P5 | SEC-2012.2.3-1 | CP-FP | Oct 2016 | http://www.p5-fp7.eu/ |
| PaaSword | ICT-07-2014 | RIA | Dec 2017 | https://www.paasword.eu/ |
| PACT | SEC-2011.6.5-2 | CP- | Jan 2015 | http://www.projectpact.eu/ |
| PANORAMIX | DS-01-2014 | IA | Aug 2018 | https://panoramix-project.eu/ |
| PARIS | SEC-2012.6.1-2 | CP-FP | Feb 2016 | http://www.paris-project.org/ |
| PASS | PEOPLE-2007 | MC | Nov 2012 | |
| PATS | SiS-2008-1.2.2.1 | CSA | Mar 2012 | |
| PICOS | ICT-2007.1.4 | CP | Jun 2011 | http://www.picos-project.eu/ |
| PQCRYPTO | ICT-32-2014 | RIA | Feb 2018 | https://pqcrypto.eu.org/ |
| PRACTIS | SiS-2009-1.1.2.1 | CP | Mar 2013 | |
| PRECIOSA | ICT-2007.6.2 | CP | Aug 2010 | |
| PRESCIENT | SiS-2009-1.1.2.1 | CP | Mar 2013 | http://www.prescient-project.eu |
| PreserviX | ICT-37-2014-1 | SME-1 | Oct 2015 | http://www.piql.com/ |
| PrEstoCloud | ICT-06-2016 | RIA | Dec 2019 | http://www.prestocloud-project.eu/ |
| PrimeLife | ICT-2007.1.4 | CP | Jun 2011 | http://primelife.ercim.eu/ |
| PRIPARE | ICT-2013.1.5 | CSA | Sep 2015 | pripareproject.eu |
| PRISM | ICT-2007.1.4 | CP | May 2010 | http://www.fp7-prism.eu/ |
| PRISM CODE | FP7-PEOPLE | MC-CIG | Oct 2016 | |
| PRISMACLOUD | ICT-32-2014 | RIA | Jul 2018 | https://prismacloud.eu/ |
| PRISMS | SEC-2011.6.5-2 | CP-FP | Jul 2015 | http://prismsproject.eu/ |
| PRIVACY FLAG | DS-01-2014 | IA | Apr 2018 | http://privacyflag.eu/ |
| Privacy.Us | MSCA | MSCA | Nov 2019 | https://privacyus.eu/ |
| PRIVACY4FOREN SICS | FP7-PEOPLE | MC | Mar 2018 | |

| | | | | |
|---------------|------------------|---------|------------|---|
| ProBOS | SMEInst-13 | SME-2 | Sep 2018 | |
| PROTECTIVE | DS-04-2015 | IA | Aug 2019 | https://protective-h2020.eu/ |
| Ps2Share | ICT-35-2016 | RIA | Dec 2017 | http://p2share.eu |
| RAPID | ICT-07-2014 | RIA | Dec 2017 | http://www.rapid-project.eu/ |
| REASSURE | DS-01-2016 | RIA | Dec 2019 | http://reassure.eu/ |
| ReCRED | DS-02-2014 | IA | Apr 2018 | http://www.recred.eu/ |
| REDSENTRY | H2020-SME1 | SME-1 | Dec 2017 | |
| RESPECT | SEC-2011.6.1-5 | CP-FP | May 2015 | http://respectproject.eu/ |
| REVEN-X1 | ICT-37-2015-1 | SME-1 | Dec 2015 | |
| SafeCloud | DS-01-2014 | IA | Aug 2018 | http://www.safecloud-project.eu/ |
| SAFEcrypto | ICT-32-2014 | RIA | Dec 2018 | https://www.safecrypto.eu/ |
| SAFERtec | DS-01-2016 | RIA | Dec 2019 | http://www.safertec-project.eu/ |
| SAINT | DS-04-2016 | RIA | Feb 2021 | https://project-saint.eu/ |
| SAURON | CIP-01-2016 | IA | Apr 2019 | https://sauronproject.eu/ |
| SCISSOR | ICT-32-2014 | RIA | Dec 2017 | https://scissor-project.com/ |
| SCOTT | ECSEL-2016 | IA | Jun 2020 | https://scottproject.eu/ |
| SCR | SMEInst | SME-1 | Dec 2016 | |
| SecIoT | INNOSUP-0 | CSA | Aug 2018 | |
| SERECA | ICT-07-2014 | RIA | Feb 2018 | https://www.serecaproject.eu/ |
| SHARCS | ICT-32-2014 | RIA | Dec 2017 | http://sharcs-project.eu/ |
| SHIELD | DS-03-2016 | RIA | 31/12/2019 | http://www.project-shield.eu/ |
| SHIELD | DS-04-2015 | IA | Feb 2019 | https://www.shield-h2020.eu/ |
| SISSDEN | DS-04-2015 | IA | Apr 2019 | https://sisssden.eu |
| SMESEC | DS-02-2016 | IA | May 2020 | |
| SocialPrivacy | FP7-PEOPLE | MC-IOF | Aug 2015 | |
| SODA | ICT-18-2016 | RIA | Dec 2019 | https://www.soda-project.eu/ |
| SPECIAL | ICT-18-2016 | RIA | Dec 2019 | https://www.specialprivacy.eu/ |
| SpeechXRays | DS-02-2014 | IA | Apr 2018 | http://www.speechxrays.eu/ |
| SPOOC | ERC-CoG-2014 | ERC-COG | Aug 2020 | |
| STAMP | ICT-10-2016 | RIA | Nov 2019 | https://www.stamp-project.eu/ |
| STOP-IT | CIP-01-2016-2017 | IA | May 2021 | https://stop-it-project.eu/ |
| STORM | EE-13-2014 | RIA | Aug 2018 | |
| SUNFISH | ICT-07-2014 | RIA | Dec 2017 | http://www.sunfishproject.eu/ |
| SUPERCLOUD | ICT-07-2014 | RIA | Jan 2018 | https://supercloud-project.eu/ |

| | | | | |
|-------------|----------------|-------|----------|---|
| SurPRISE | SEC-2011.6.5-2 | CP-FP | Jan 2015 | http://surprise-project.eu/ |
| SysSec | ICT-2009.1.4 | NoE | Nov 2014 | http://www.syssec-project.eu/ |
| TREADOR | ICT-16-2015 | RIA | Dec 2018 | http://www.treador-project.eu/ |
| TREDISEC | ICT-32-2014 | RIA | Mar 2018 | http://www.tredisec.eu/ |
| TRUESSEC.EU | DS-01-2016 | CSA | Dec 2018 | https://truessec.eu/ |
| TYPES | DS-01-2014 | IA | Oct 2017 | http://www.types-project.eu/ |
| U2PIA | SMEInst-13 | SME-1 | Mar 2017 | |
| UNICORN | ICT-06-2016 | IA | Dec 2019 | http://unicorn-project.eu/ |
| VESSEEDIA | DS-01-2016 | RIA | Dec 2019 | https://vessedia.eu/ |
| VIRT-EU | ICT-35-2016 | RIA | Dec 2019 | https://virteuproject.eu/ |
| VisiOn | DS-01-2014 | | Jun 2017 | http://www.visioneuproject.eu/ |
| WISER | DS-06-2014 | IA | Nov 2017 | http://cyberwiser.eu/ |
| WITDOM | ICT-32-2014 | RIA | Dec 2017 | http://www.witdom.eu/ |


ANNEX B. PRESENTATION GIVEN TO JOINT MEETING ON TAXONOMY ALIGNMENT.



A suggested taxonomy of cybersecurity to support clustering of EU and national cybersecurity research projects to enable peer-to-peer learnings

Prof. David Wallom


Funded by the European Commission
Horizon 2020 - Grant # 740219



Cybersecurity

EQUIPMENT PEOPLE

“Cyber security consists of technologies, processes and measures that are designed to protect systems, networks and data from cyber crimes.”



Clustering


- Bring together EC and if possible national projects to ensure rich sharing of outputs and best practices,
- Assess each projects affinity to taxonomy components,
- Apply repeatable unsupervised machine learning techniques to these data as evidence-based characterisation of the cybersecurity landscape,
- Use resampling of the dataset and replacement to enable bootstrapping analysis to validate taxonomy.

Cybersecurity Research Taxonomy

- Foundational technical methods & risk management for trustworthy systems in cybersecurity & privacy
- Applications and user-oriented services to support cybersecurity and privacy
- Policy, governance, ethics, trust, and usability, human aspects of cybersecurity & privacy.

Cybersecurity Research Taxonomy

- Secure Systems and Technology
- Operational Risk and Analytics
- Identity, Behaviour and Ethics
- National and international security and governance
- Verification and Assurance
- Human Aspects of Cybersecurity



Secure Systems and Technology

- Building Security & privacy into technology from the design stage and technologies that are designed to deliver security capabilities, examples include;
 - Cryptography,
 - Trusted platforms,
 - Wireless & mobile security,
 - Cloud Computing security,
 - Secure software development/coding paradigms.

Operational Risk and Analytics

- Developing understanding of risk and harm resulting from cyberattack;
 - cyberattack propagation across and between organisations,
 - awareness of current understanding of scenario and risk management,
 - Metrics and models for security postures,
 - Analytics for predicting risk, prioritising responses and supporting security operations.

Identity, Behaviour, Ethics and Privacy

- Management of personal identity including different levels of assurance when used for online capabilities or services,
- How to understand common norms when applied in the online or digital realm,
- Diverse perspectives and interpretations to questions such as;
 - Who are you online with?
 - How do you communicate, and what can (or should) you do?
 - What expectations (personal and legally binding) are there? E.g. directives?
- What expectations of privacy can there be and should there be?

National and international security and governance

- Development of Politics, international relations, defence, policy and governance issues
 - How do countries and communities interact with (and through) technology, and how might this change in different contexts?
 - How do national standards transcend borders or boundaries?
 - How should different threat persistence levels and domain cybersecurity understanding be shared?
 - At what point does something change from being a business problem to a national security problem?

Verification and Assurance

- Enabling the establishment of levels of confidence in a system in terms of security and privacy, primarily looking at other systems to either determine if they are secure or to assert they are;
 - Formal Verification seeks to build a mathematical model of a digital system and then try to prove whether it is 'correct', often helping to find subtle flaws,
 - Assurance focuses on managing risks related to the use, processing, storage, and transmission of information.

Human Aspects of Cybersecurity

- Understanding humans interaction with, and through, digital systems;
 - whether to understand and design for target users,
 - understand how adversaries operate and can exploit the systems.
- Includes aspects like usability, trust, collaborative practices, social embeddedness, nationhood, cultural diversity and the relationship between microsocial interactions and global structures.

Clustering mechanism from Model

- 4 technical development areas
- 2 Social or service based cross cutting areas
- Projects score themselves from 1 (least) to 5 (most) as to how important this area is to developments ongoing within the project.
- Projects will then be clustered using both Principle component analysis and Heirical clustering on the resulting scores from projects that have engaged.
- Initially to create base dataset Cyberwatching members will score projects they are investigating using Service Offerings as basis.

Fitting to other models

- There are of course other models of CS available, both general and domain specific
- Then lets compare...

NIST Critical Infrastructure Cybersecurity Framework

- **Identify**
 - Asset Management
 - Business Environment
 - Governance
 - Risk Assessment
 - Risk Management Strategy
- **Protect**
 - Access Control
 - Awareness and Training
 - Data Security
 - Information Protection Processes and Procedures
 - Maintenance
 - Protective Technology
- **Detect**
 - Anomalies and Events
 - Security Continuous Monitoring
 - Detection Processes
- **Respond**
 - Response Planning
 - Communications
 - Analysis
 - Mitigation
 - Improvements
- **Recover**
 - Recovery Planning
 - Improvements
 - Communications

<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

EC Glossary for Cybersecurity

| Domain | Description |
|---|---|
| Assurance, Audit and Certification | This domain refers to the methodologies, frameworks and tools that provide ground for having confidence that a system or network is working or has been designed to operate as the desired security target or according to a defined security policy. |
| Cryptology | Cryptology groups together Cryptography and Cryptanalysis. |
| Data Security and Privacy | This domain includes security and privacy issues related to data in order to (a) reduce by design privacy and confidentiality risks without impairing data processing purposes or (b) by processing purpose of data after it is accessed by authorized entities. The learning process of acquiring knowledge, know-how, skills and/or competences necessary to protect network and information systems, their users, and affected persons from cyber threats. |
| Education and Training | This domain refers to the theories, techniques, tools and processes for the identification, collection, acquisition and preservation of digital evidence that can be of evidential value. |
| Operational Incident Handling and Digital Forensics | This domain includes the interplay between ethics, relevant laws, regulations, policies, standards, psychology and the human being within the cybersecurity realm. |
| Human Aspects | This domain covers security concerns related to the authentication, access control and authorization of individuals and smart objects (their associated operations). |
| Identity and Access Management (IAM) | This domain refers to the governance activities, methodologies, processes and tools aimed at the management of cyber risks. |
| Security Management and Governance | This domain encompasses the scientific and methodological competences related to the interplay between cybersecurity networks and hybridized systems. |
| Network and Distributed Systems | This domain comprises security aspects in the software and hardware development lifecycle and covers them such as risk and requirements analysis, architecture design, code implementation, code auditing, validation, verification, testing, deployment, runtime monitoring, etc. operation and certification. |
| Software and Hardware Security Engineering | Information security measures and indicators are used to facilitate decision making and improve performance and accountability through the collection, analysis and reporting of relevant performance-related data. |
| Security Measurements | This domain refers to the legal and ethical aspects related to the misuse of technology. It is distribution and/or reproduction of material covered by intellectual property rights and the enforcement of law related to cybercrime and digital rights. |
| Technology and Legal Aspects | This domain refers to the use of formal analysis and verification techniques to provide theoretical proof of security properties either in software, hardware and algorithm design. |
| Theoretical Foundations of Security Analysis and Design | This domain comprises trust issues related to digital and physical entities such as applications, services, components, or systems. Trust management approaches can be employed in order to provide assurance and accountability guarantees. |
| Trust Management, Assurance, and Accountability | |

EC Glossary for Cybersecurity

- Operational Incident Handling and Digital Forensics
- Security Measurements
- Assurance, Audit and Certification
- Theoretical Foundations of Security Analysis and Design
- Cryptology
- Network and Distributed Systems
- Software and Hardware Security Engineering
- Identity and Access Management (IAM)
- Technology and Legal Aspects
- Trust Management, Assurance, and Accountability
- Data Security and Privacy
- Education and Training
- Security Management and Governance
- Human Aspects

Validation

- Utilise bootstrapping and dataset resampling to ensure stastically sound results.

Conclusions to clusters

- Broad categories allow for projects to consider themselves how they understand a categories meaning
- Fewer simple categories likely to generate clusters of projects with critical mass
- Ensuring that the projects score themselves will ensure they are accurately representing what they are doing