Council of the
European Union

Brussels, 20 September 2018
(OR. en)

12104/18
ADD 4

Interinstitutional File:
2018/0328(COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	12 September 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2018) 403 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

Delegations will find attached document SWD(2018) 403 final.

Encl.: SWD(2018) 403 final

EUROPEAN
COMMISSION

Brussels, 12.9.2018
SWD(2018) 403 final

PART 4/4

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 404 final}

European Commission

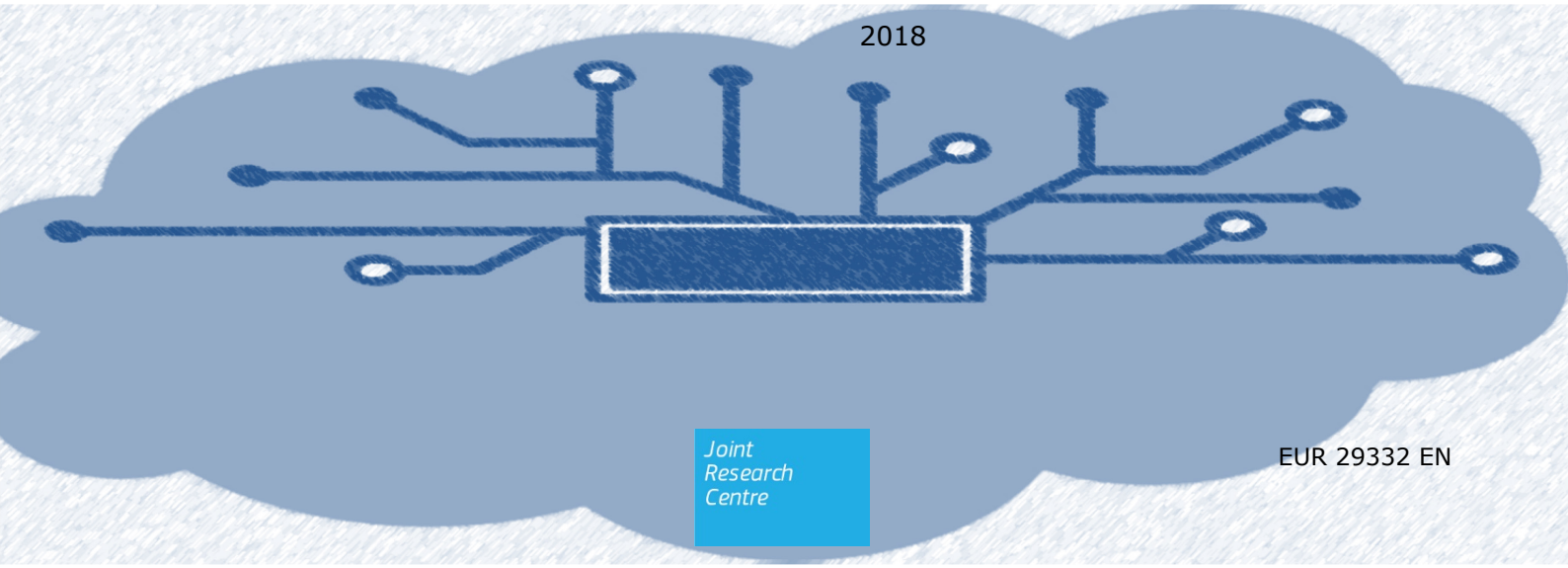
JRC TECHNICAL REPORTS

European Cybersecurity Centres of Expertise Map

Definitions and Taxonomy

NAI-FOVINO, I.
NEISSE, R.
LAZARI, A.
RUZZANTE, G.
POLEMI, N.
FIGWER, M.

2018



Joint Research Centre

EUR 29332 EN

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

JRC Science Hub
https://ec.europa.eu/jrc

EUR 29332 EN

JRC 111441

PDF ISBN 978-92-79-92956-4 ISSN 1831-9424 doi: 10.2760/622400

Luxembourg: Publications Office of the European Union, 2018

© European Union, 2018

The reuse policy of the European Commission is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Reuse is authorised, provided the source of the document is acknowledged and its original meaning or message is not distorted. The European Commission shall not be liable for any consequence stemming from the reuse. For any use or reproduction of photos or other material that is not owned by the EU, permission must be sought directly from the copyright holders.

All content © European Union 2018

How to cite this report: NAI-FOVINO, I.; NEISSE, R.;'LAZARI, A.; RUZZANTE, G.; POLEMI, N.; FIGWER, M. European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy. EUR 29332 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-92956-4, doi: 10.2760/622400, JRC111441.

Contents

Abstract ..... **Error! Bookmark not defined.**

1 Introduction ..... **Error! Bookmark not defined.**

2 Methodology and Reference Sources analysis ..... **Error! Bookmark not defined.**

2.1 Methodology ..... **Error! Bookmark not defined.**

2.2 Reference Sources and State of the Art..... **Error! Bookmark not defined.**

2.2.1 Existing cybersecurity clustering approaches**Error! Bookmark not defined.**

2.2.1.1 Cyberwatching..... **Error! Bookmark not defined.**

2.2.1.2 ACM Classification System..... **Error! Bookmark not defined.**

2.2.1.3 NIST CSRC Taxonomy ..... **Error! Bookmark not defined.**

2.2.1.4 IEEE Taxonomy ..... **Error! Bookmark not defined.**

2.2.1.5 ETSI TC-Cyber working group domains **Error! Bookmark not defined.**

2.2.1.6 IFIP TC11 Working Groups taxonomy... **Error! Bookmark not defined.**

2.2.1.7 IT-baseline protection catalog (IT-Grundschutz) ..**Error! Bookmark not defined.**

2.2.2 International Standards and Reference documents ....**Error! Bookmark not defined.**

2.2.2.1 ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27005 ..**Error! Bookmark not defined.**

2.2.2.2 ISA 62443 ..... **Error! Bookmark not defined.**

2.2.2.3 ISO/IEC 15408 (Common Criteria) ..... **Error! Bookmark not defined.**

2.2.2.4 NIST SP 800..... **Error! Bookmark not defined.**

2.2.3 International Working Groups and Organisations .....**Error! Bookmark not defined.**

2.2.4 Regulations and Policy Documents..... **Error! Bookmark not defined.**

2.2.5 Cybersecurity Market Studies and Observatory Initiatives .**Error! Bookmark not defined.**

2.2.6 General Considerations on the analysed sources.....**Error! Bookmark not defined.**

3 A Holistic Taxonomy for Cybersecurity Research Domains .....**Error! Bookmark not defined.**

3.1 Cybersecurity Domains..... **Error! Bookmark not defined.**

3.1.1 Assurance, Audit, and Certification ..... **Error! Bookmark not defined.**

3.1.2 Cryptology (Cryptography and Cryptanalysis) .....**Error! Bookmark not defined.**

3.1.3 Data Security and Privacy ..... **Error! Bookmark not defined.**

3.1.4 Education and Training ..... **Error! Bookmark not defined.**

3.1.5 Operational Incident Handling and Digital Forensics ...**Error! Bookmark not defined.**

3.1.6 Human Aspects ..... **Error! Bookmark not defined.**
3.1.7 Identity and Access Management (IAM) ..... **Error! Bookmark not defined.**
3.1.8 Security Management and Governance ..... **Error! Bookmark not defined.**
3.1.9 Network and Distributed Systems..... **Error! Bookmark not defined.**
3.1.10 Software and Hardware Security Engineering.....**Error! Bookmark not defined.**
3.1.11 Security Measurements ..... **Error! Bookmark not defined.**
3.1.12 Legal Aspects ..... **Error! Bookmark not defined.**
3.1.13 Theoretical Foundations ..... **Error! Bookmark not defined.**
3.1.14 Trust Management, Assurance, and Accountability.....**Error! Bookmark not defined.**
3.2 Sectorial Dimensions..... **Error! Bookmark not defined.**
3.2.1 Audiovisual and media..... **Error! Bookmark not defined.**
3.2.2 Defence..... **Error! Bookmark not defined.**
3.2.3 Digital Infrastructure ..... **Error! Bookmark not defined.**
3.2.4 Energy ..... **Error! Bookmark not defined.**
3.2.5 Financial..... **Error! Bookmark not defined.**
3.2.6 Government and public authorities ..... **Error! Bookmark not defined.**
3.2.7 Health ..... **Error! Bookmark not defined.**
3.2.8 Maritime..... **Error! Bookmark not defined.**
3.2.9 Nuclear ..... **Error! Bookmark not defined.**
3.2.10 Public Safety ..... **Error! Bookmark not defined.**
3.2.11 Tourism..... **Error! Bookmark not defined.**
3.2.12 Transportation..... **Error! Bookmark not defined.**
3.2.13 Smart Ecosystems ..... **Error! Bookmark not defined.**
3.2.14 Space ..... **Error! Bookmark not defined.**
3.2.15 Supply Chain..... **Error! Bookmark not defined.**
3.3 Applications and Technologies Dimension..... **Error! Bookmark not defined.**
4 Final Remarks..... **Error! Bookmark not defined.**
Annex 1 –Glossary of terms ..... **Error! Bookmark not defined.**
List of figures ..... **Error! Bookmark not defined.**

Abstract

The Commission made a commitment in the Communication adopted in September to launch a pilot phase under Horizon 2020 to help bring national cybersecurity centres together into a network. In this context, the goal of this document is that of aligning the cybersecurity terminologies, definitions and domains into a coherent and comprehensive taxonomy to facilitate the categorisation of EU cybersecurity competencies.

1 Introduction

The Commission made a commitment in the Communication adopted in September to launch a pilot phase under Horizon 2020 to help bring national cybersecurity centres together into a network. The first step of this ambitious initiative is the clear definition of the cybersecurity context, its domains of application, research and knowledge. In this context, the goal of this document is that of aligning the cybersecurity terminologies, definitions and domains to allow the categorisation and mapping of existing EU cybersecurity centres (e.g. research organisations, laboratories, associations, academic institutions, groups, operational centres, etc.) according to their cybersecurity expertise in specific domains.

For the purpose of this document **cybersecurity** is considered an interdisciplinary domain. This starting point finds support in the Cybersecurity Report issued by the High Level Advisory Group of the EC Scientific Advice Mechanism in March 2017, where it is stated clearly that:

> "*cybersecurity is not a clearly demarcated field of academic study that lends itself readily to scientific investigation. Rather, cybersecurity combines a multiplicity of disciplines from the technical to behavioural and cultural. Scientific study is further complicated by the rapidly evolving nature of threats, the difficulty to undertake controlled experiments and the pace of technical change and innovation. In short, cybersecurity is much more than a science*".

This definition implies that there is not available today a globally accepted and standardised definition of cybersecurity and a clear identification of its domain of development and of application. In this report, after an initial reflection on the different dimensions of the cybersecurity domain, and using as sources some of the most widely accepted standards, international working group classification systems, regulations, best-practices, and recommendations in the cybersecurity domain, a high level set of definitions and categorisation domains are proposed so that they:

- can be used by the EC cybersecurity initiatives;
- become a point of reference for the cybersecurity activities (research, industrial, marketing, operational, training, education) in the DSM by all sectors/industries (health, telecom, finance, transport, space, defence, banking etc.);
- can be used to index the cybersecurity research entities (e.g. research organisations/laboratories/ associations/academic institutions/groups, operational centres*/academies*) in Europe;
- *meet compliance* with international cybersecurity standards*;*
- *can be* sustainable, easily modifiable and extensible.

This report is organised as follows: Section 2.1 presents the methodology adopted to build the Cybersecurity taxonomy, illustrating each step. Section 2.2 presents instead the information sources used to build the taxonomy together with their analysis including a summary of the main concepts that emerged from the analysis. Section 3 presents in detail the proposed taxonomy. Annex 1 provides, based on international standards, definitions and terms of references for the concepts used in the taxonomy.

2 Methodology and Reference Sources analysis

This section presents the methodology that has been adopted to build the taxonomy presented in Section 3, the reference sources which have been taken into consideration (i.e. the state of the art in the domain), and the aggregation of the comparison analysis among these sources.
The details of each single reference source analysed are instead provided in Annex 1.

2.1 Methodology

Taxonomy is defined as "*the practice of classification of things or concepts, including the principles that underlie such classification*"[1].

One of things to bear in mind about taxonomies is that there is never one uniquely valid taxonomy for a given domain, but that taxonomy might be more representative and expressive than another in a given context.

The traditional approach to the definition of a taxonomy follows a number of well-defined steps (as showed in Figure 1):

(1) **Define subject scope**: this phase consists in the identification of the scope of the taxonomy (i.e. the purpose for which the taxonomy is created). In this case the scope as described in the introduction, is that of providing a clear definition of the cybersecurity context, its domains of application, research and knowledge to be used to be used to facilitate the establishment of a cybersecurity competence network;

(2) **Identify sources**: selection of sources that are widely recognised and adopted by the scientific and technological community. In this case they have been identified through desktop research taking into consideration standards, activities performed by existing international working groups and organisations, scientific literature (see Section 2.2);

(3) **Collect terms and concepts:** Each of the identified sources has been analysed to extrapolate:

   a. Relevant concepts and sub-domains;

   b. Terminology (i.e. the building blocks of every taxonomy);

(4) **Group similar concepts together:** concepts have then been clustered (see Figure 5. High-level overview of the concepts and vocabularies emerged from the analysis

(5) **Add other term relationships and details**: to identify communalities and to simplify the structure of the taxonomy. The identified terms have instead been used to build a glossary using as definitions' source international standards (where available), or scientific references.

[1] http://km4ard.cta.int/2016/11/27/developing-a-taxonomy-for-agriculture-and-rural-development/

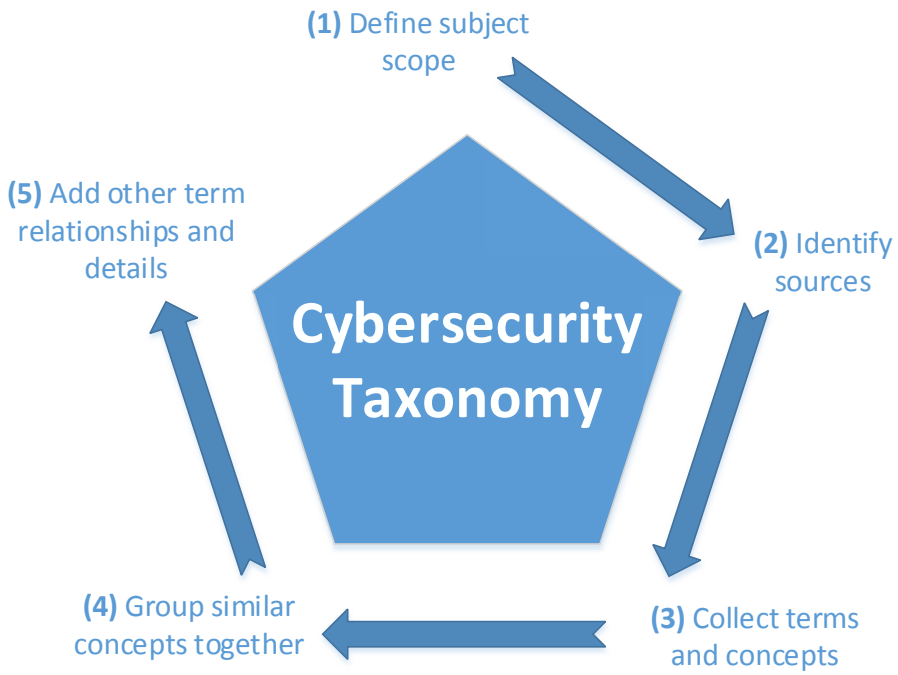


Figure 1. Cybersecurity taxonomy definition steps.

The resulting corpus of knowledge has been then structured in a three dimensional Taxonomy as described in Section 3 and validated against the few existing taxonomy covering at least a portion of the cybersecurity domain already identified among the sources.

2.2 Reference Sources and State of the Art

This section summarises steps (2) and (3) presented in section 2.1. It takes stock of existing concepts and terminologies to define a unifying, holistic and forward-looking cybersecurity taxonomy that takes into consideration at the same time:

- Existing cybersecurity clustering activities;
- International Standards and Reference documents;
- International Working Groups results/activities;
- Regulations and policy initiatives;
- Cybersecurity Market studies and Observatory initiatives.

In what follows, for each of the listed sources the state of the art is presented.

2.2.1 Existing cybersecurity clustering approaches

As already mentioned in the introduction, due to the heterogeneous nature of the cybersecurity domain, a uniquely accepted and consolidated taxonomy does not exist in the literature. Many organisations however defined their own taxonomy tailored for their own specific needs. The following subsections describe the most structured and comprehensive approaches identified in the literature.

2.2.1.1 Cyberwatching

The *European observatory of research and innovation in the field of cybersecurity and privacy* (Cyberwatching)[2] is an initiative falling under the *Coordination and Support Action* scheme aiming at "*defining and promoting a pragmatic approach to implement*

[2] https://www.cyberwatching.eu

and maintain an EU Observatory to monitor R&I initiatives on cybersecurity & privacy, throughout EU & Associated Countries".

To support its activities, Cyberwatching defined a taxonomy of cybersecurity composed by four vertical technical development areas, which are complemented by two horizontal service-based cross cutting cybersecurity clusters (see the following figure). Their goal is to use this taxonomy with a score system to cluster European Research and Innovation initiatives dealing with cybersecurity and privacy where entities can position themselves by assigning a value from 1 to 5 as to how important each area is to developments ongoing within each of their ongoing projects.

Figure 2. Vertical and horizontal cybersecurity development areas

Moreover, it created a catalogue of European Projects on cybersecurity organised according to two dimensions:

Characteristics	Vertical Markets
• Cloud security • Collaborative platform • Cyber security • Privacy • Big Data	• Digital Health • Energy • Engineering & manufacturing • Finance & insurance • ICT • Local & public administrations • National government agencies • Smart cities

Table 1. European Projects Catalogue dimensions

The areas identified by Cyberwatching are aligned with those identified by NIST (Section 2.2.1.3) and, partially, with those of ETSI (Section 2.2.1.5). The taxonomy proposed in this report is also in alignment with the areas defined by the EU Cyberwatching, however, additional horizontal dimensions are considered addressing the sector of actuation, and the target applications and technologies.

2.2.1.2 ACM Classification System

The Association for Computing Machinery (ACM) proposed a Computing Classification System (CCS)[3] that includes **Security and privacy** as a top generic area. The first version was created in 1998 and the latest version was updated on 2012. The purpose of the CCS is to classify publications submitted to ACM events and published in the ACM digital library, which is considered one of the main global sources of high quality peer-reviewed scientific publications. The following table summarizes the main categories and sub-categories for the Security and privacy top generic area:

[3] https://dl.acm.org/ccs/ccs.cfm

Cryptography • Key management • Public key (asymmetric) techniques: • Digital signatures • Public key encryption • Symmetric cryptography and hash functions • Block and stream ciphers • Hash functions and message authentication codes • Cryptanalysis and other attacks • Information-theoretic techniques • Mathematical foundations of cryptography	**Formal methods and theory of security** • Trust frameworks • Security requirements • Formal security models • Logic and verification	**Security services** • Authentication • Biometrics • Graphical / visual passwords • Multi-factor authentication • Access control • Pseudonymity, anonymity and untraceability • Privacy-preserving protocols • Digital rights management • Authorization
Intrusion/anomaly detection and malware mitigation • Malware and its mitigation • Intrusion detection systems • Artificial immune systems • Social engineering attacks • Spoofing attacks • Phishing	**Security in hardware** • Tamper-proof and tamper-resistant designs • Embedded systems security • Hardware security implementation • Hardware-based security protocols • Hardware attacks and countermeasures • Malicious design modifications • Side-channel analysis and countermeasures • Hardware reverse engineering	**Systems security** • Operating systems security • Mobile platform security • Trusted computing • Virtualization and security • Browser security • Distributed systems security • Information flow control • Denial-of-service attacks • Firewalls • Vulnerability management • Penetration testing • Vulnerability scanners • File system security
Network security • Security protocols • Web protocol security • Mobile and wireless security • Denial-of-service attacks • Firewalls	**Database and storage security** • Data anonymization and sanitization • Management and querying of encrypted data • Information accountability and usage control • Database activity monitoring	**Human and societal aspects of security and privacy** • Economics of security and privacy • Social aspects of security and privacy • Privacy protections • Usability in security and privacy
Software and application security • Software security engineering • Web application security • Social network security and privacy • Domain-specific security and privacy architectures • Software reverse engineering		

Table 2. ACM Classification System Categories

This taxonomy covers in an extensive way the traditional academic research sub-domains of cybersecurity, while it does not cover the more operational subdomains, such as cybercrime forensics, assurance, certification, auditing, standardisation and the legislative angle. Moreover, it does not capture sectorial specific competences.

2.2.1.3 NIST CSRC Taxonomy

NIST Computer Security Resource Centre (CSRC)[4], which is an important reference resource of NIST for what concerns cybersecurity, defined a comprehensive model for clustering cybersecurity knowledge. NIST adopts a multidimensional clustering approach based on six cross-cutting areas of classification:

- Security and privacy specific research domains;
- Technologies (where the research is performed);
- Applications (field of application of the knowledge);
- Laws and regulations;

[4] https://csrc.nist.gov/topics

- Type of activities;
- Business sectors.

Table 3 provides a view of the second-level classification taxonomy. As it is possible to see it covers explicitly some aspects not fully addressed by the others taxonomies, in particular for what concerns the application fields, the sectorial specific competencies, laws and regulations.

Security and Privacy	**Technologies**	**Applications**
cryptography	big data	cyber-physical systems
general security & privacy	biometrics	cybersecurity education
identity & access management	Basic Input/Output System	cybersecurity framework
privacy	cloud & virtualization	cybersecurity workforce
risk management	communications & wireless	forensics
security & behavior	databases	industrial control systems
security measurement	firewalls	Internet of Things
security programs & operations	firmware	small & medium business
Laws and Regulations	hardware	supply chain
executive documents	mobile	telework
laws	networks	voting
regulations	operating systems	**Sectors**
Activities and Products	personal computers	energy
annual reports	sensors	financial services
conferences & workshops	servers	healthcare
reference materials	smart cards	hospitality
standards development	software	manufacturing
	storage	public safety
		retail
		transportation

Table 3. Cybersecurity Topic Clustering (NIST Computer Security Resource Center)

While on a side this approach is very well structured, it is important to note how (a) it doesn't capture some peculiarities of the European landscape (e.g. in the Law and Regulation context, in the sectors identified etc.), and (b) the number of dimensions to take into considerations which is so large to risk to introduce a high fragmentation in clustering of competencies.

Nevertheless, this classification is, to the best of our knowledge, the most articulated and precise and was taken as one of the main starting points to elaborate in Section 3 the taxonomy fit for the purpose of this report.

2.2.1.4 IEEE Taxonomy

Following a similar approach as ACM, the Institute of Electrical and Electronics Engineers (IEEE) also proposes a taxonomy[5] with the same purpose, to categorize the publications of events that are made available through the IEEE Xplore Digital Library. The following list summarizes the main concepts and sub-categories of this taxonomy:

- **Access control**: Authorization, Capability-based security
- **Computer security:** Authentication, Computer crime, Computer hacking, Firewalls (computing), Identity management systems, Permission

[5] 2017 IEEE Taxonomy: https://www.ieee.org/documents/taxonomy_v101.pdf last access 06/12/2017

- **Cryptography:** Ciphers, Encryption, Public key, Quantum cryptography, Random number generation, Side-channel attacks;
- **Data security:** Cryptography, Message authentication; Digital signatures;
- **Information security**: Intrusion detection; Network security; Power system security; Reconnaissance; Security management;
- **Terrorism:** Bioterrorism, National security; Watermarking

Similarly to the ACM taxonomy, the IEEE taxonomy covers in general all the traditional technical academic (sub-)domains of cybersecurity, however, is significantly more concise and less comprehensive since little emphasis is put on relevant aspects such as privacy and data protection (covered here only by "data security", but limited to cryptographic methods), on sectorial applications and obviously on social and legal aspects. Standards, certification, economic aspects, law implication and cyber-crime are not clustered as well as sectorial specific competences. Nevertheless, this taxonomy, allows anyway to validate the taxonomy of NIST and complements it regarding some second level concepts.

2.2.1.5 ETSI TC-Cyber working group domains

The European Telecommunications Standards Institute (ETSI) established a technical committee[6] dedicated to the development of standards to increase privacy and security for organizations and citizens across Europe and worldwide. The TC covers a set of domains that can be taken as input in the definition of a taxonomy of cybersecurity taking into consideration industry interests (see Table 4).

Horizontal cybersecurity	Securing technologies and systems	Security tools and techniques
• Privacy by design • Security controls • Network and Information Security • Critical infrastructures • Information Security Indicators	• Mobile/Wireless systems (3G/4G, TETRA, DECT, RRS, RFID...) • IoT and Machine-to-Machine (M2M) • Network Functions Virtualisation • Intelligent Transport Systems, Maritime • Broadcasting	• Lawful Interception and Retained Data • Digital Signatures and trust service providers • Secure elements • Exchangeable CA/DRM solutions • Cryptography

Table 4. ETSI TC-Cyber working group domains

Moreover, ETSI presents an overview of the Global Cyber Security Ecosystem defining a short glossary of cybersecurity definitions, an analysis of the basic cybersecurity components, and an extensive survey of the main worldwide entities working on the field. There is no inventory of the respective actuation areas, only a list defined by entity type (e.g., standardization body, research institute, centres of excellence, forums, etc.).
For the purposes of a cybersecurity classification scheme the components are an important cross-cutting dimension that should be taken into consideration from a cybersecurity management perspective, for example, companies may specialize on protection, detection, or recovery after an incident (see **Error! Reference source not found.**).

[6] http://www.etsi.org/technologies-clusters/technologies/cyber-security

Figure 3. ETSI cross-cutting cybersecurity clusters

2.2.1.6 IFIP TC11 Working Groups taxonomy

The International Federation for Information Processing[7] (IFIP) is a non-governmental, non-profit umbrella organization for national societies working in the field of information processing. It was established in 1960 under the auspices of UNESCO as a result of the first World Computer Congress held in Paris in 1959. Among its Technical Committees (TC), of particular interest is TC11 on Security and Privacy Protection in Information Processing Systems[8].

The TC11 committee is organised in thematic working groups (see Figure 4). The structure and content of the thematic groups can be indeed considered as a sort of embryonic cybersecurity and privacy taxonomy (definitions and vocabulary are obviously missing as the structure of the TC was not meant to be considered as a real taxonomy).

[7] http://ifip.org/
[8] https://www.ifiptc11.org/

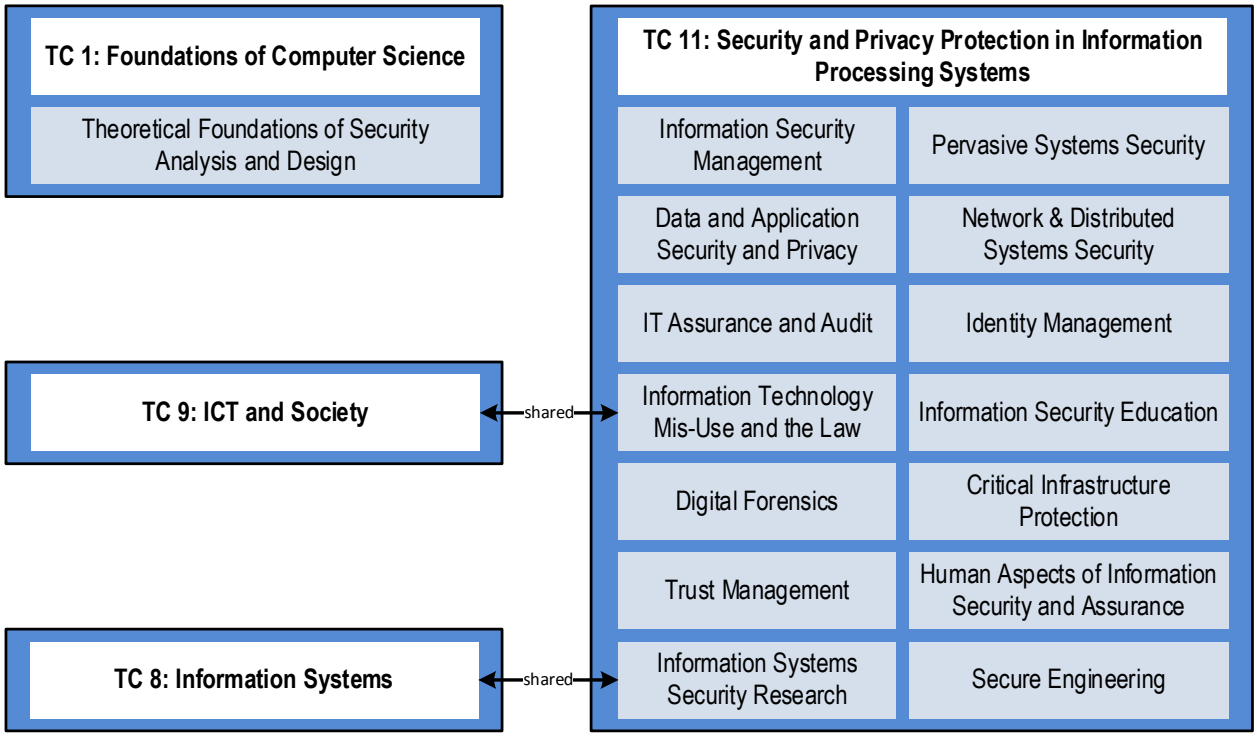


Figure 4. IFIP TC 11 Structure

In the following table a summary of the different field of application of the working groups is presented.

WG 1.7 - Theoretical Foundations of Security Analysis and Design • Formal definition and verification of the various aspects of security, confidentiality, integrity, authentication and availability; • New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their manifold applications (e.g., electronic commerce); • Information flow modelling and its application to the theory of confidentiality policies, composition of systems, and covert channel analysis; • Formal techniques for the analysis and verification of mobile code; • Formal analysis and design for prevention of Denial of Service (DoS).	**WG 11.1 Information Security Management** • Upper management awareness on information security • Managerial aspects concerning information security • Assessment of information security effectiveness and degree of control by managers; • Risk analysis • Identification of threats and vulnerabilities • Measurement and assessment of security levels in a company • Identification of the impact of hardware and software changes on the management of Information Security; • Technical aspects; • Standards for Information Security; • Disaster recovery.	**WG 11.2 Pervasive Systems Security** • Information security particularly related to pervasive systems

WG 11.3 Data and Application Security and Privacy • Statement of security and privacy requirements for data management systems; • Design, implementation, and operation of data management systems that include security and privacy functions; • Assurance that implemented data management systems meet their security and privacy requirements.	**WG 11.4 Network & Distributed Systems Security** • Management and technicians awareness in respect of the reliable and secure operation of the information networks; • Education and training in the application of security principles, methods, and technologies to networking; • Network aspect of information systems security; • Managerial, procedural and technical aspects of network security; • Requirements for network security; • Network oriented cybersecurity risk analysis; • Network security controls	**WG 11.5 IT Assurance and Audit** No detailed information was available about this working group.
WG 11.6 Identity Management • Identity management • Biometric technologies • National identity management	**WG 11.7 / 9.6 Information Technology Misuse and Law** No detailed information was available about this working group.	**WG 11.8 IT Security Education** • Education and training in information security. • Courses in information security at the university level; • Business educational training on information security modules • Collection, exchange and dissemination of information relating to information security courses conducted by private organizations for industry; • Collection and periodical dissemination of annotated bibliography of information security books, feature articles, reports, and other educational media.
WG 11.9 Digital Forensics • Theories, techniques and tools for extracting, analyzing and preserving digital evidence; • Network and cloud forensics; • Embedded device forensics; • Digital forensic processes and workflow models; • Digital forensic case studies; WG 11.9 Digital Forensics • Theories, techniques and tools for extracting, analyzing and preserving digital evidence; • Network and cloud forensics; • Embedded device forensics; • Digital forensic processes and workflow models; • Digital forensic case studies; • Legal, ethical and policy issues related to digital forensics.	**WG 11.10 Critical Infrastructure Protection** • Infrastructure vulnerabilities, threats and risks; • Security challenges, solutions and implementation issues; • Infrastructure sector interdependencies and security implications; • Risk analysis, risk assessment and impact assessment methodologies; • Modeling and simulation of critical infrastructures; • Legal, economic, policy and human factors issues related to critical infrastructure protection; • Secure information sharing; • Infrastructure protection case studies; • Distributed control systems/SCADA security; • Telecommunications network security;	**WG 11.11 Trust Management** • Semantics and models for security and trust; • Trust management architectures, mechanisms and policies; • Trust in e-commerce, e-service, e-government; • Trust and privacy; • Identity and trust management; • Trust in securing digital as well as physical assets; • Social and legal aspects of trust.

WG 11.12 Human Aspects of Information Security and Assurance	WG 11.13 / 8.11 Information Systems Security Research	WG 11.14 Secure Engineering
• Information security culture; • Awareness and education methods; • Enhancing risk perception; • Public understanding of security; • Usable security; • Psychological models of security software usage; • User acceptance of security policies and technologies; • User-friendly authentication methods; • Automating security functionality; • Non-intrusive security; • Assisting security administration; • Impacts of standards, policies, compliance requirements; • Organizational governance for information assurance; • Simplifying risk and threat assessment; • Understanding motivations for misuse; • Social engineering and other human-related risks; • Privacy attitudes and practices; • Computer ethics and security.	• Theoretical and empirical analyzes of information security behaviour; • Adoption, use, and continuance of information security technologies and policies; • Compliance with information security and privacy policies, procedures, and regulations; • Investigations of computer crime and security violations; • Motivators and inhibitors of employee computer crime; • Forensic analysis of security breaches and computer crimes; • Individual, organizational, and group information privacy concerns and behaviors; • Legal, societal, and ethical issues in information security; • investigations of information security behaviour (Neurosecurity).	• Security requirements engineering with emphasis on identity, privacy and trust: • Secure Service Architectures and Design: • Security support in programming environments • Service composition and adaptation: • Risk and Cost-aware Secure Service Development: • Security assurance for services: • Quantitative security for assurance

Table 5. IFIP WG 11 Research sub-groups

The organisation of the TC11 clearly cannot be considered a formal and complete taxonomy. It reflects existing groups of interest and research communities. This explains why it contains several redundancies and it results unbalanced in term of deepness. Nevertheless, it provides the most extensive collection of concepts and topics analysed in this report and it constitutes without doubts a good starting point for the definition of a general taxonomy of the cybersecurity domain.

2.2.1.7 IT-baseline protection catalog (IT-Grundschutz)

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) proposed the IT Baseline Protection (IT-Grundschutz) methodology to support the identification and implementation of cybersecurity measurements in organizations. In addition to the methodology BSI also provides an extensive catalogue (IT-Grundschutz Catalogue) of threats and countermeasures including a glossary of terms.

This catalogue is organized considering the components, threats, and measures. The component catalogue is organized in the following layers: general aspects, infrastructure, IT systems, networks, and IT applications. Each component layer targets a specific group in the organization, for example, management, technicians, system administrators, users, network administrators, etc.

This classification and separation in target groups makes it easy to find the relevant information and guidance when using the catalogue. For the purposes of a cybersecurity classification scheme this layered structure is useful and is also reflected in the topics proposed by the NIST Computer Security Resource Center.

2.2.2 International Standards and Reference documents

Under this group goes all the standards and documents helping in building the basic building block of a taxonomy, i.e. the glossary of definitions. To make an example under this category fall all the ISO/IEC standards. (see the following subsections for a detailed list)

The following standards have been taken into consideration to build the taxonomy proposed in Section 3.

ISO/IEC 2382	ISO/IEC 24760	**ISO/IEC 27032**	ISO/TS 12812-2

ISO/IEC 5127	ISO/IEC 25010	ISO/IEC 27033	ISO/IEC 15408 (Common Criteria)
ISO/IEC 9735	ISO/IEC 25237	ISO/IEC 27037	ISA 62443
ISO/IEC 10118	ISO/IEC 27000	ISO/IEC 28000	NIST SP 800
ISO/IEC 10181	ISO/IEC 27001	ISO/IEC 29100	NIST SP 800 55
ISO/IEC 11770	ISO/IEC 27002	ISO/IEC 29109-1	NISTIR 8105
ISO/IEC 11889	ISO/IEC 27004	ISO/TR 18307	ETSI:tr (cyber)
ISO/IEC 18033	ISO/IEC 27005	ISO/TR 11633-2	
ISO/IEC 23006-4	ISO/IEC 27019	ISO/TS 80004	

Table 6. List of Standards taken into consideration

Some of the listed international standards are strictly related with the cybersecurity realm. It is important however to underline that in general these standards have been conceived for some very specific certification or procedural task and not to describe or define the cybersecurity ecosystem. However, they can in any case be considered as an important reference source for cybersecurity vocabularies, glossaries and, in some case, very specific domains (e.g. information security management for what concerns ISO/IEC 27000, 27001, 27005).

The description of the content of all the mentioned standards is out of the scope of this report. The majority of them has been used to cover some specific vocabulary definition (see the glossary at the end of the report). A little subsection however has been used much more extensively, not only as source for the glossary, but also to identify specific concepts and domains of the taxonomy and for that reason in the following a more detailed description is provided.

2.2.2.1 ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27005

These standards provide the ground for the definition and implementation of an Information Security Management System (ISMS) with an architecture similar to several others ISO/IEC standards such as ISO/IEC 9000 and ISO/IEC 14000.

ISO/IEC 27000 provides definitions and vocabulary for the cybersecurity context, which can be used as one of the sources for the glossary of the categorisation presented in this report. ISO/IEC 27001 and ISO/IEC 27005 as they provide the description of a specific domain of the cybersecurity realm, the ISMS and the Cybersecurity Risk Assessment process which merit to be included in the set of knowledge clusters proposed in Section 3.

2.2.2.2 ISA 62443

The 62443 series of standards have been developed jointly by the ISA99 committee and IEC Technical Committee 65 Working Group 10 (TC65WG10) to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS).

The goal in applying the 62443 series is to improve the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, including the procurement aspects. The 62443 series builds on established standards for the security of general purpose information technology systems (e.g., the ISO/IEC 27000 series), differentiating from the 27000 mainly for what concerns (a) some additional aspects as safety, health and environment (not present in ISO/IEC 27001 and ISO/IEC 27005), and (b) for some additional terms and definitions. Of interest for this report is in particular the ISA 62443-1-2 technical report containing a master glossary of terms and abbreviations used throughout the series.

2.2.2.3 ISO/IEC 15408 (Common Criteria)

Standard containing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.
The standard is composed by three parts:

- **Part 1, Introduction and general model**: is the introduction to ISO/IEC 15408. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation;
- **Part 2, Security functional requirements**: establishes a set of functional components as a standard way of expressing the functional requirements for TOEs (Targets Of Evaluation);
- **Part 3, Security assurance requirements**: establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs.

Each part of the standard contains a catalogue of components (mostly functional) tackling different aspects of the cybersecurity functional and assurance requirements. However, as for the others standards analysed so far, this catalogue is instrumental to the specific scope of the Common Criteria, hence it is too specific to be taken as reference for a taxonomy of the cybersecurity knowledge.

2.2.2.4 NIST SP 800

NIST maintains a series of "Special Publications" (SP) on cybersecurity best practices related to cybersecurity. This collection of publications is extremely practical and each issue is devoted to a particular, technical domain (spanning from security guidelines to LTE, to cybersecurity education etc.).

Hence, for the purposes of this report, the NIST SP 800 is not very useful as it is too much specialised. However, the NIST Computer Security Resource Center, which is the reference resource of NIST for what concerns cybersecurity, defined a model for clustering cybersecurity knowledge extremely interesting and comprehensive, which can be taken as reference.

2.2.3 International Working Groups and Organisations

International working groups have been taken as additional sources for reference definitions, or, in some case to analyse the structure of the sub-working groups to extrapolate the related taxonomy. Here below a summarising list is provided[9].

- *Association for Computing Machinery (ACM)*: see Section 2.2.1.2
- *National Institute of Standards and Technology (NIST)*: see Section 2.2.1.3
- *Institute of Electrical and Electronics Engineers (IEEE)*: see Section 2.2.1.4
- *European Telecommunications Standards Institute (ETSI)*: see Section 2.2.1.5
- *International Federation for Information Processing (IFIP)*: see Section 2.2.1.6

The following sources have been taken into consideration as a source for the glossary on this report:

- Internet Engineering Task Force (IETF): Request for Comments (RFC) 4949[10] "Internet Security Glossary, Version 2" produced by the Network Working Group;
- Intel Threat Agent Library (TAL)[11] and Threat Agent Motivation[12];

[9] Contributions coming from ACM, NIST, IEEE, ETSI AND IFIP have been already described in the previous sub-sections, hence, to avoid information redundancy, in the following list the related entries will only point to the proper sub-section.
[10] https://tools.ietf.org/html/rfc4949
[11] https://communities.intel.com/docs/DOC-23853

- MACE Taxonomy, Adversary Types[13];
- CAPEC ATT&CK from Mitre[14];
- Cyber Kill Chain[15];

- *Open Web Application Security Project Foundation (OWASP)*: OWASP is a worldwide not-for-profit charitable organization focused on improving the security of software. The corpus of definitions available on the OWASP portal[16] has been taken into consideration to cover definition gaps in the glossary on this report.

- *Information Systems Audit and Control Association (ISACA)*: ISACA has been used as source of definitions and references for what concerns the information security governance aspects, in particular leveraging on the ISACA "*cybersecurity fundamentals glossary"*[17]

- *European Union Agency for Network and Information Security (ENISA)*: ENISA has a very active role in the European Cybersecurity ecosystem. Among its large portfolio of activities, is worth mentioning the release of cybersecurity related reports and studies. In particular, for the purposes of this report, have been taken into consideration as relevant sources

  - "Definition of Cybersecurity, Gaps and overlaps in standardisation", ENISA report, December 2015
  - "Review of Cyber Hygiene practices", ENISA report, December 2016
  - "An evaluation Framework for National Cyber Security Strategies", ENISA report, November 2014
  - "EP3R 2013 – Position Paper Task Forces on Terminology Definitions and Categorisation of Assets (TF-TDCA)", December 2013
  - "Recommended cryptographic measures - Securing personal data", ENISA report, November 2013

  Incident taxonomies collected by ENISA under the CSIRT initiative[18] have also been taken into consideration, as well as the ENISA and NIS WG3 cybersecurity education map.

- *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE):* The NATO CCD COE is a multinational and interdisciplinary hub of cyber defence expertise. The Centre organises the world's largest and most complex international technical cyber defence exercise Locked Shields and the annual conference on cyber conflict, CyCon. Of particular interest for what concerns the definition of a cybersecurity taxonomy, is the International Cyber Developments Review (INCYDER) database. This interactive research tool focuses on the legal and policy documents adopted by international organisations active in cyber security. The collection of documents is periodically updated and supported by a comprehensive system of tags that enable filtering the content by specific sub-domains.

---

[12] https://lists.oasis-open.org/archives/cti/201607/msg00044/Intel_Corp_Threat_Agent_Motivations_Feb2015.pdf
[13] http://cradpdf.drdc-rddc.gc.ca/PDFS/unc218/p803340_A1b.pdf
[14] https://attack.mitre.org/mobile/index.php/Main_Page
[15] https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html
[16] https://www.owasp.org/index.php/Glossary accessed in November 2017
[17] http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf accessed in November 2017
[18] https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies accessed in November 2017.

- *European Cyber Security Organisation (ECSO)*: it represents the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity.
    - In its Industry proposal[19] ECSO has elaborated an analysis of the following different class of market solutions/services:
        - Governance, vulnerability and cybersecurity management;
        - Identity and access management;
        - Data security;
        - Cloud Security;
        - Applications security;
        - Network systems security;
        - Hardware (device/endpoint) security;
        - Audit, planning and advisory services;
        - Management and operations services;
        - Managed Security Services (MSS);
        - Security training services.
    - The activities of ECSO are organised around 6 working groups:
        - WG1: Standardisation, certification, labelling and supply chain management
        - WG2: Market deployment, investments and international collaboration
        - WG3: Sectoral demand
        - WG4: Support to SMEs, coordination with countries (in particular East and Central EU) and regions
        - WG5: Education, awareness, training, exercises
        - WG6: Strategic Research and Innovation Agenda (SRIA)

      Of particular interest for the scope of this report are WG5 and WG6.

2.2.4 **Regulations and Policy Documents**

European Regulation and policy documents were considered as sources for legal definitions and to cover the gaps left by the vocabularies extracted from standards when dealing with non-technical definitions. Here below the list of the most relevant taken into consideration:

- DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS directive)
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)
- European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cybersecurity (2011/2284(INI)) (CIIP)
- COM(2017) 477 final 2017/0225 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity

[19] http://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf

Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

- COM(2016) 705 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Space Strategy for Europe
- JOIN(2014) 9 final - JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL For an open and secure global maritime domain: elements for a European Union maritime security strategy
- JOIN(2016) 18 final JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response
- EU Cyber Defence Policy Framework [Consilium 15585/14] and Joint Communication on 'Cybersecurity
- Strategy of the European Union: An Open, Safe and Secure Cyberspace', February 2013 [JOIN(2013)1].

Several of these regulations and policy documents are related to specific sectors, and have been used to understand the position occupied by cybersecurity and privacy in a specific policy sector. However two of these policy documents (NIS and GDPR) can be considered overarching and cross-sectorial and have been used in the taxonomy presented in Section 3 as relevant sources to identify regulatory and sectorial sub-domains.

2.2.5 **Cybersecurity Market Studies and Observatory Initiatives**

Observatory initiatives and market studies have been used to capture taxonomy aspects related to the industry and business world.

- *PWC and LSEC Cybersecurity Industry Market Analysis study:* this study, analyses the European cybersecurity industry. Within the study data related to the EU industry is clustered according the following cybersecurity categories:
    - Anti-Malware;
    - Application Security;
    - Business Continuity;
    - Cyber Consultancy;
    - Cyber Insurance;
    - Encryption;
    - Identity and Access Control;
    - Infrastructure;
    - Mobile;
    - Outsourced/Managed Services;
    - Situational Awareness;
    - System Recovery.

  This list provides a good market oriented overview, which validates several of the key-domains already emerged in the analysis of the others sources. However it does not fully cover the research, regulatory and sectorial domains.
- *Security Research Map (SEREMA):* The purpose of the Security Research Map is to increase the visibility of security related research in Europe and to optimize the networking between research facilities, universities, public authorities, end users, suppliers of security solutions and operators of critical infrastructures. Serema contains the profiles of universities, research centres and companies that are

active in the field of security with the aim of creating a network among those that are interested in forming a consortium for H2020 or similar funding schemes. The database has been developed within the network of National Contact Points for Security in the 7th EU-Framework Programme (SEREN 2). The classification scheme adopted is in line with those identified so far.

- *Cyber Growth Partnership (CGP)*: CGP is a UK initiative aiming to provide oversight and give strategic guidance to the government on supporting the development of the UK cyber security ecosystem. Within the CGP, the Cyber Exchange is an online platform enabling participants across industry, academia and government to list news, events and resources.
- *Cyberwatching.eu: see Subsection 2.2.1.1.*

2.2.6 General Considerations on the analysed sources

The sources presented in the previous section have been used to identify:

- A common set of vocabularies and terms;
- A set of specific sub-domains;
- A set of applicative sectors.

Ad-hoc desktop research activities have been conducted to identify relationships among domains, synonyms and to discriminate between cybersecurity peculiarities and generic items. Table 7 summarises the contribution provided by all the identified sources to the definition of the taxonomy presented in section 3, while Figure 1 and Figure 5 provides a high-level overview of the concepts and vocabularies emerged from the analysis described in this section.

On the basis of the analysis conducted, it is possible to draw some general considerations:

- The analysed standards provided a good source reference for the definition of terms, and for the identification of some domain areas linked to the risk-assessment domain. The same risk-assessment elements can be found in the resilience function areas defined by NIST and well as in the NIST CSRC categorisation. When instead coming to the identification of research domains, the analysed standards can be considered negligible as conceived to drive a technical standardisation process in very specific domains and not to classify knowledge and scientific activities
- The NIS directive and the NIST CRSC share, with some variations, a common understanding of the sectors where cybersecurity must be considered paramount, hence by merging these two sectorial views it is possible to identify a relevant element of the taxonomy which will be presented in Section 3
- The taxonomies of IEEE, IFIP, ECSO, ETSI and Cyberwatch.eu often overlap with the NIST CRSC resulting the better detailed and logically structured. The merging of these three sources could provide a good starting point for what concerns the technological and scientific domains.
- NIST CRSC considers into its categorisation also law and regulation aspects; this is perfectly in line with the scope of the taxonomy subject of this study, however the sub-domains listed are obviously related to the US regulation landscape, and cannot be considered as useful to map the EU law and regulation cybersecurity expertise. However, the NIS directive and the GDPR can be used there to close the gap

As it is possible to see the identified sources well complement each other allowing to cover almost all the cybersecurity spectrum.

By using the identified concepts and leveraging on standards for what concerns definitions and vocabulary, a more general and EU oriented taxonomy of the cybersecurity and privacy domain is presented in Section 3.

Source	General concepts	Academic Research	Regulatory	Operational	Sectorial	Application	Economic and Business	Social	Standards	Vocabulary
Cyberwatching	x	x		x						
ACM Classification System	x	x				x	x	x		
NIST CSRC Taxonomy	x	x	x	x	x	x	x	x		
IEEE	x	x								
ETSI TC-Cyber	x	x		x					x	
IFIP WG 11	x	x				x	x	x		
IT-Grundschutz	x	x				x				
International Standards (Section 2.2)	x		x	x	x	x			x	x
OWASP	x									x
ENISA	x		x	x	x					x
ECSO	x					x	x			
EU Regulations (Section 2.2.4)	x		x	x	x	x		x	x	x
PWC Study						x	x			
SEREMA						x	x			
CGP						x	x			

Table 7. Sources contributions to the Cybersecurity Taxonomy

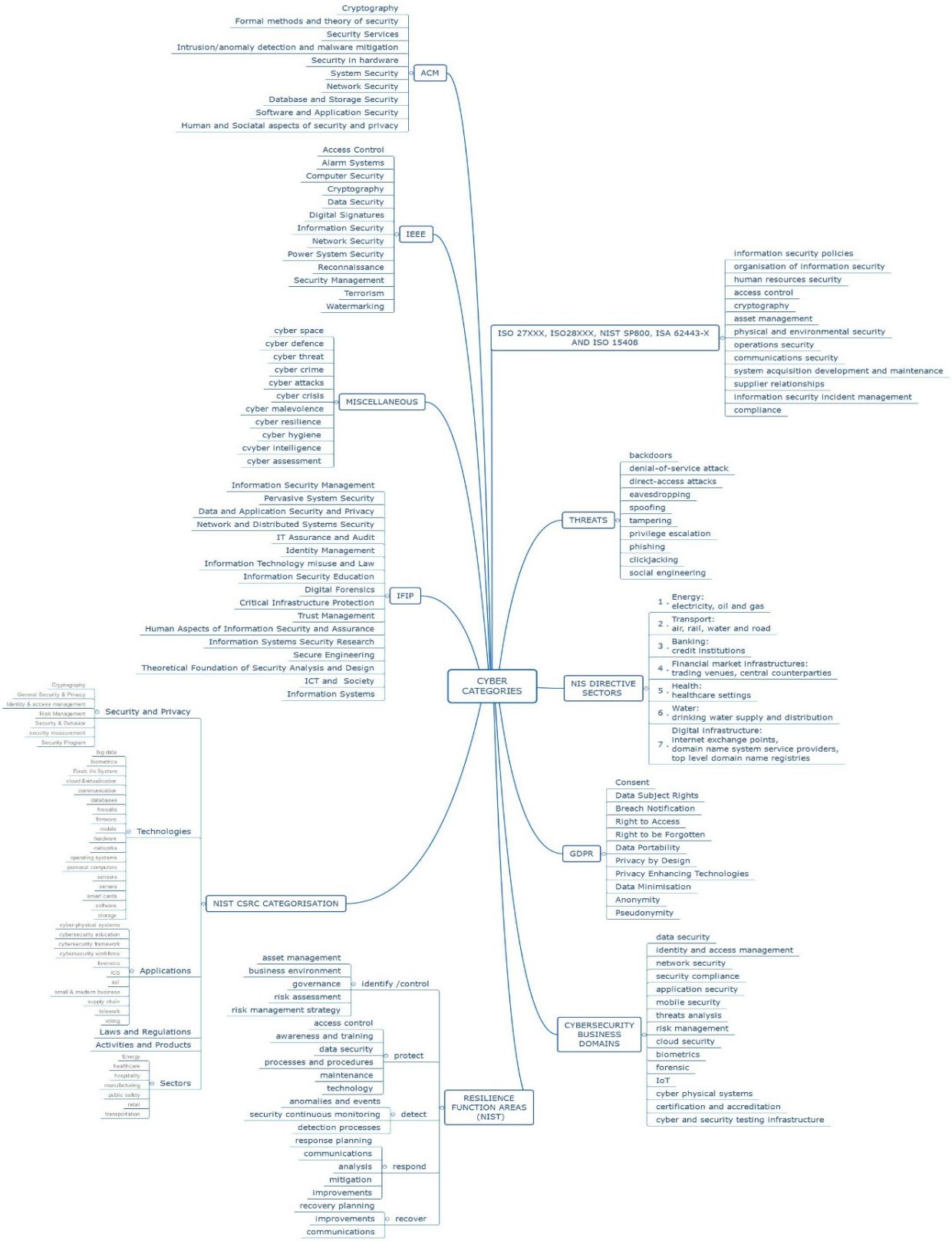


Figure 5. High-level overview of the concepts and vocabularies emerged from the analysis

3 A Holistic Taxonomy for Cybersecurity Research Domains

The analysis of the reference sources described in the previous section highlights the complexity and heterogeneity of the cybersecurity discipline. In a similar situation, in order to ensure capturing every aspect of this domain, the taxonomy proposed in this document might risk to become super-specialised, with a multitude of nested domains. The goal of the taxonomy proposed in this report is that of supporting the mapping of the European cybersecurity competencies available.

The analysis conducted so far however suggests adopting a different, more agile approach. The analysis of the scientific/technological working groups activities (e.g. IFIP, ETSI etc.) and of the "knowledge management entities" (e.g. ACM, IEEE etc.) gives a clear and precise indication of the **areas of fundamental research** within the cybersecurity domain. On the other side, the analysis of policy documents and regulations allowed to magnify which **sectorial domains** are perceived as the most relevant for the wellbeing of the European Society (the assumption here is that regulations and policy packages answer to a precise European citizen and industry regulatory needs). Finally, the analysis of the market studies, of the observatory initiatives and of the R&D programs (H2020), provides an indication of the field of **technological applications** of the cybersecurity foundational research results.

This reasoning reached the conclusion that a taxonomy trying to cluster a complex and multifaceted discipline as cybersecurity needs to be structured on multiple dimensions, capturing not only the core and traditional research domains, but also impacted sectors and applications. Figure 6, depicts, in a graphical way, the proposed three-dimensional taxonomy, based on the following dimensions:

- Cybersecurity domains;
- Sectors (to protect which applications, technologies and cybersecurity research are developed and used);
- Applications and Technologies (on which the cybersecurity research results are applied).

Each dimension has been fine-tuned and detailed on the basis of the analysis presented in the previous section to:

a) ensure its alignment with the European Regulatory landscape;
b) ensure its comprehensiveness (merging together where needed sub-domains highlighted in different classifications and standards);
c) avoid redundancy of terms and definitions.

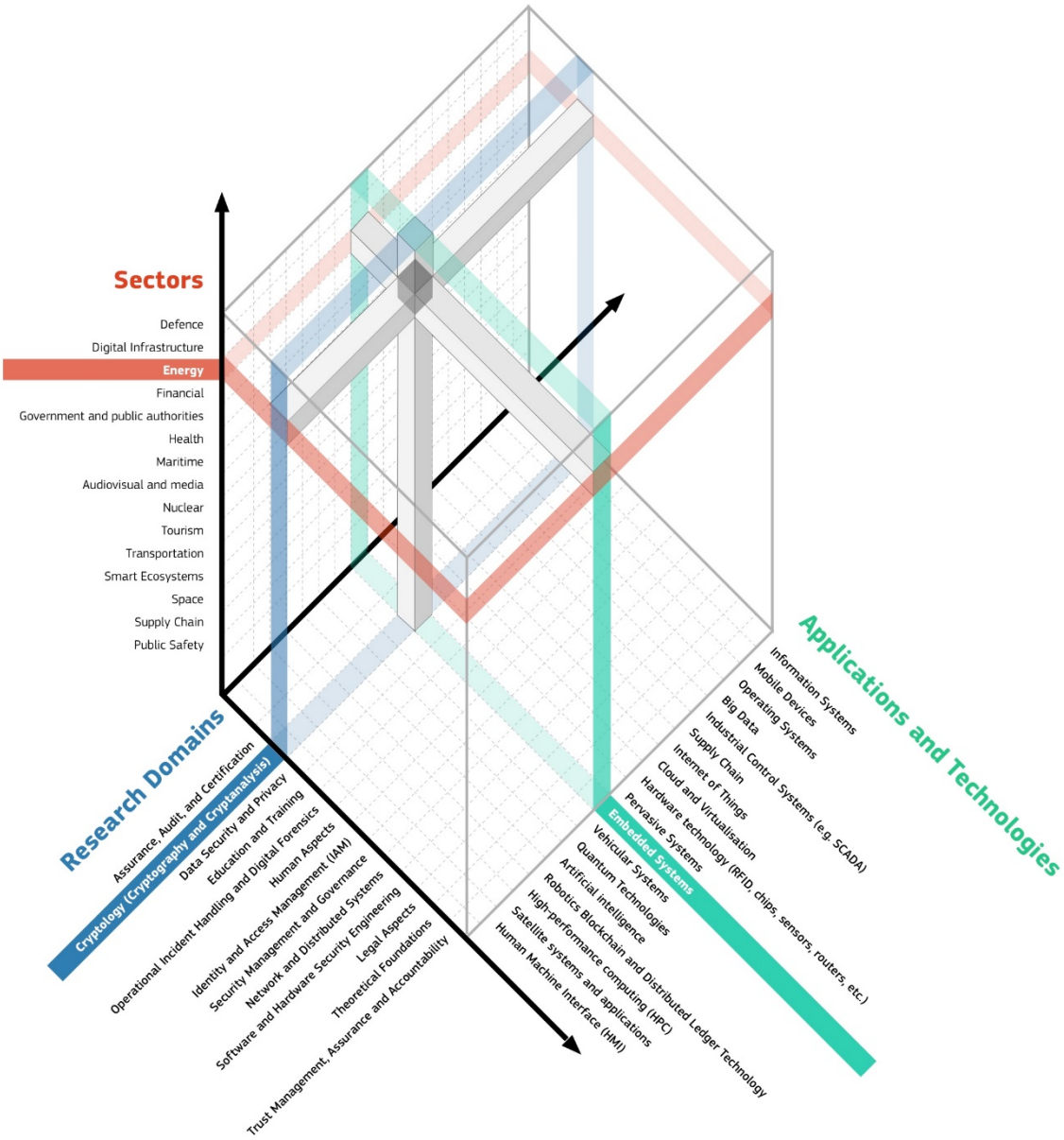


Figure 6. High Level view of the Cybersecurity Taxonomy

In what follows, definitions for each dimension of the proposed taxonomy are presented. More in details, Subsection 3.1 lists for each of cybersecurity domains the relevant sub-domains. Subsection 3.2 details the sectorial sub-domains, and Subsection 3.3 illustrates the list of applications and technologies. The taxonomy is completed with the glossary of concepts and vocabulary included in Annex 1. The cybersecurity subdomains defined for each domain, sectors, applications, and technologies are by no means an **exhaustive list**, these elements will be complemented in the future based on the input from cybersecurity centre of excellences surveyed.

3.1 Cybersecurity Domains

The following subsections provides a definition for each cybersecurity domain and lists the respective subdomains.

3.1.1 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 at the desired security target or according to a defined security policy.

- Assurance;
- Audit;
- Assessment;
- Certification;
- Protection Profile;
- Security Target.

3.1.2 Cryptology (Cryptography and Cryptanalysis)

Cryptology groups together by definition of Cryptography and Cryptanalysis. For the scope of this taxonomy, under this sub-domain fall the mathematical aspects of cryptology, the algorithmic aspects, their technical implementation and infrastructural architectures as well as the implementation of cryptanalytic methodologies, techniques and tools.

- Digital signatures;
- Asymmetric cryptography and cryptanalysis;
- Symmetric cryptography and cryptanalysis;
- Hash functions;
- Key management;
- Message authentication;
- Random number generation;
- Cryptanalysis methodologies, techniques and tools;
- Quantum cryptology;
- Post-quantum cryptology;
- Mathematical foundations of cryptography;
- Steganography.

3.1.3 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 preventing misuse of data after it is accessed by authorized entities.

- Privacy requirements for data management systems;
- Design, implementation, and operation of data management systems that include security and privacy functions;
- Pseudonymity;
- Unlinkability;
- Privacy by design and Privacy Enhancing Technologies (PET);
- Digital Rights Management (DRM);
- Data usage control.

3.1.4 Education and Training

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

- Cybersecurity education;
- Cybersecurity aware culture;

- Cybersecurity simulation platforms;
- Cybersecurity exercises;
- Cybersecurity ranges;
- Cybersecurity education methodology;
- Cybersecurity vocational training;
- Certification Programmes.

3.1.5 Operational Incident Handling and Digital Forensics

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.

- Incident analysis & Documentation;
- Containment Strategy design;
- Forensic evidence collection;
- Tracking/Tracing;
- Incident response;
- Vulnerability analysis & response;
- Artifact analysis & response;
- Digital evidence preservation;
- Incident forecasting (intelligence based);
- Digital forensic processes and workflow models;
- Digital forensic case studies;
- Legal, ethical and policy issues related to digital forensics.

3.1.6 Human Aspects

The interplay between ethics, relevant laws, regulations, policies, standards, psychology and the human being within the cybersecurity realm.

1. Accessibility;
2. Usability;
3. Social engineering and other human-related risks;
4. Socio-technical security;
5. Human errors;
6. Enhancing risk perception;
7. Psychological models;
8. User acceptance of security policies and technologies;
9. Automating security functionality;
10. Non-intrusive security;
11. Individual, organizational, and group information privacy concerns and behaviours;
12. Motivators and inhibitors of insider misuse;
13. Impacts of standards, policies, compliance requirements;
14. Organizational governance for information assurance;
15. Social engineering and other human-related risks;
16. Privacy attitudes and practices;
17. Computer ethics and security;
18. Transparent security;
19. Attacker profiling;
20. Security Psychology;
21. Legal and Regulatory Issues.

3.1.7 Identity and Access Management (IAM)

This domain covers authentication,authorization and access control of individuals and smart objects when accessing resources. These concerns may include

physical and digital elements of authentication systems and legal aspects related to compliance and law enforcement.

- Identity management models, frameworks, services (e.g. identity federations, single-sign-on, Public Key Infrastructure) ;
- Authentication/Access Control Technologies (X509 certificates, RFIDs, biometrics, PKI smart cards, SRAM PUF etc.)
- Protocols and frameworks for IAM;
- Identity management quality assurance;
- electronic IDentification, Authentication and trust Services (eIDAS);
- Optical and electronic document security;
- Legal aspects of identity management;
- Law enforcement and identity management.

3.1.8 Security Management and Governance

Governance and management activities, methodologies, processes and tools aimed at the preservation of confidentiality, integrity and availability of information as well as other properties such as authenticity, accountability and non-repudiation [SOURCE ISO/IEC 27000].

- Risk management;
- Continuous monitoring;
- Threats and vulnerabilities modelling;
- Attack modelling and countermeasures;
- Managerial aspects concerning information security
- Assessment of information security effectiveness and degrees of control;
- Identification of the impact of hardware and software changes on the management of Information Security;
- Standards for Information Security;
- Incident management and disaster recovery;
- Reporting (e.g. disaster recovery and business continuity)
- Theoretical and empirical analyses of information security behaviour;
- Adoption, use, and continuance of information security technologies and policies;
- Compliance with information security and privacy policies, procedures, and regulations;
- Vetting for security staff and employees;
- Economic aspects of the cybersecurity ecosystem;
- Vulnerability Assessment and Penetration Testing (VAPT);
- Attack prevention and detection;
- Capability Maturity Models.

3.1.9 Network and Distributed Systems

Network security is concerned with hardware, software, basic communication protocols, network frame structure, and communication mechanisms factors of the network. [SOURCE ISO/IEC TR 29181-5]. Information Security in the network context deals with data integrity, confidentiality, availability and non-repudiation while is sent across the network. A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages [3]. In this context cybersecurity deals with all the aspects of computation, coordination, message integrity, availability and (if required) confidentiality. Message authentication is also in the scope.

- Network security (principles, methods, protocols, algorithms and technologies);
- Distributed Systems Security;
- Managerial, procedural and technical aspects of network security;

- Protocols and frameworks for secure distributed computing;
- Network layer attacks and mitigation techniques;
- Network attack propagation analysis;
- Distributed systems security analysis and simulation;
- Distributed consensus techniques;
- Fault tolerant models;
- Secure distributed computations;
- Auditability and Accountability;
- Honey nets and Honey Pots.

3.1.10 Software and Hardware Security Engineering

Security aspects in the software and hardware development lifecycle such as risk and requirements analysis, architecture design, code implementation, validation, verification, testing, deployment and runtime monitoring of operation.

- Security requirements engineering with emphasis on identity, privacy, accountability, and trust;
- Security and risk analysis of components compositions;
- Secure software architectures and design;
- Security design patterns;
- Secure programming principles and best practices;
- Security support in programming environments;
- Security documentation;
- Refinement and verification of security management policy models;
- Runtime security verification and enforcement;
- Continuous monitoring;
- Security testing and validation;
- Vulnerability discovery and penetration testing;
- Quantitative security for assurance;
- Intrusion detection and honeypots;
- Malware analysis;
- Model-driven security and domain-specific modelling languages;
- Self-healing systems;
- Side Channel Attacks (e.g. Power attacks, Electromagnetic Radiation attacks, etc.);
- Fault Injection Attacks.

3.1.11 Security Measurements

Information security measures are used to facilitate decision making and improve performance and accountability through the collection, analysis and reporting of relevant cybersecurity performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements [SOURCE NIST SP800-55].

- Security analytics and indicators;
- Security metrics;
- Validation and comparison frameworks for security metrics;
- Measurement and assessment of security levels.

3.1.12 Legal Aspects

This domain refers to the legal and ethical aspects related to the misuse of technology, illicit distribution and/or reproduction of material covered by IPR and the enforcement of law related to cybercrime and digital rights.

- Cybercrime prosecution and law enforcement;

- Cybersecurity and ethics;
- Intellectual property rights;
- Cybersecurity regulation analysis and design;
- Investigations of computer crime (cybercrime) and security violations;
- Legal, societal, and ethical issues in information security;
- Legal aspect of certification;
- Social media (e.g. fake news).

3.1.13 Theoretical Foundations

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. Formal verification is the act of proving or disproving the correctness of intended algorithms underlying a system with respect to a certain formal specification or property, using formal methods of mathematics.

- Formal specification and verification of the various aspects of security;
- Formal techniques for the analysis, verification and auditing of software and hardware;
- Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis;
- New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications;
- Formal Verification of security assurance.

3.1.14 Trust Management, Assurance, and Accountability

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.

- Semantics and models for security, accountability, privacy, and trust;
- Trust management architectures, mechanisms and policies;
- Trust and privacy;
- Identity and trust management;
- Trust in securing digital as well as physical assets;
- Trust in decision making algorithms;
- Trust and reputation of social and mainstream media;
- Social and legal aspects of trust;
- Reputation models;
- Trusted computing.

3.2 Sectorial Dimensions

The following subsections list sectors and subsectors proposed for cybersecurity taxonomy.

3.2.1 Audiovisual and media

- Broadcasting;
- Publishing;
- Internet.

3.2.2 Defence

- Aeronautics;
- Space;
- Electronics;

- Land systems;
- Telecomm;
- Shipbuilding;
- Cyber defence;
- Dual-use cybersecurity technologies;
- Critical Information Infrastructures (CIIs).

3.2.3 Digital Infrastructure

- IXPs;
- DNS service providers;
- TLD name registries;
- Telecomm Infrastructures.

3.2.4 Energy

- Electricity;
- Distribution system operators;
- Transmission system operators;
- Energy Production Operators;
- Energy prosumers;
- Energy Third party services;
- Smart meters and equipment;
- Energy CIIs;
- Oil;
- Operators of oil transmission pipelines;
- Operators of oil production;
- Refining and treatment facilities, storage and transmission;
- Gas;
- Distribution system;
- Transmission system operators;
- Storage system operators;
- LNG system operators and services;
- Natural gas undertakings;
- Operators of natural gas refining and treatment facilities;
- Green Energy.

3.2.5 Financial

- Credit institutions;
- Operators of trading venues;
- Central counterparties (CCPs);
- Banking services;
- Insurance services;
- Financial CIIs;
- Brokerage services.

3.2.6 Government and public authorities

- Data collection;
- eGovernment systems and services;
- Law enforcement;
- Governmental CIIs.

3.2.7 Health

- Health care settings (including hospitals and private clinics);
- Healthcare supply chain;
- Medical devices industrial sector;

- Pharmaceutical industry;
- e/m Health;
- Helath CIIs.

3.2.8 Maritime

- Surveillance services;
- Border control services;
- Environmental protection;
- Fisheries;
- Port Authorities
- Port services;
- Maritime supply chains.

3.2.9 Nuclear

- Radiation protection;
- Transport of radioactive substances and waste;
- Waste management;
- Safeguarding nuclear materials;
- Safety of nuclear installations;
- Nuclear research and training activities.

3.2.10 Public Safety

- Fire services;
- Rescue services;
- Medical services;
- Police;
- Emergency communications;
- Civil protection;
- Inspections services;
- First Responders.

3.2.11 Tourism

- Accommodation;
- Food and Beverage Services;
- Recreation and Entertainment Infrastructures and Services;
- Travel Services.

3.2.12 Transportation

- Air transport;
- Air carriers;
- Airport managing bodies;
- Automotive industry;
- Traffic management control operators;
- Rail transport;
- Infrastructure managers;
- Railway undertakings;
- Water transport;
- Inland, sea and coastal passenger and freight water transport companies;
- Managing bodies of ports;
- Operators of vessel traffic services;
- Road transport;
- Road authorities;
- Operators of Intelligent Transport Systems;
- Sea transport;

- Container Ships;
- Passenger's Ships- Cruise Lines;
- Fisheries;
- Multi modal transport;
- Transport CIIs.

3.2.13 Smart Ecosystems

- Smart infrastructures (e.g. Industry 4.0);
- Smart (cities, vehicles, infrastructures, objects);
- Smart environments;
- Smart governance;
- Smart energy;
- Smart Networks (e.g. Home Networks).

3.2.14 Space

- Space industry;
- Satellite operators, including ground based stations;
- Positioning and timing information;
- Navigation services;
- Earth observation;
- Satellite data providers, including data storage.

3.2.15 Supply Chain

- Natural resources;
- Raw materials;
- Components;
- Retails.

3.3 Applications and Technologies Dimension

The following list details, as described at the begin of this section, the applications and technology dimensions:

- Artificial intelligence;
- Big Data;
- Blockchain and Distributed Ledger Technology (DLT);
- Cloud and Virtualisation;
- Embedded Systems;
- Hardware technology (RFID, chips, sensors, routers, etc.);
- High-performance computing (HPC);
- Human Machine Interface (HMI);
- Industrial Control Systems (e.g. SCADA);
- Information Systems;
- Internet of Things;
- Mobile Devices;
- Operating Systems;
- Pervasive Systems;
- Quantum Technologies;
- Robotics;
- Satellite systems and applications;
- Supply Chain;
- Vehicular Systems.

4 Final Remarks

The goal of this document is that of aligning the cybersecurity terminologies, definitions and domains to allow the categorisation of existing EU cybersecurity centres (e.g. research organisations/laboratories/ associations/academic institutions/groups, operational centres) according to their cybersecurity expertise in specific domains.

Due to the intrinsically multifaceted nature of cybersecurity the accomplishment of a similar task required an "horizontal, cross-silos effort" to collate, organise and integrate existing classifications with the goal of defining a comprehensive cybersecurity taxonomy not limited to the traditional academic research domain, but able to transversal capture competencies, concepts and definitions.

The resulting three-dimensional taxonomy presented in Section 3 is not static, but it is open to modifications and must be understood as a living semantic structure which will change during the years to keep the pace of the fast evolution of the digital world.

Annex 1 –Glossary of terms

Accessibility

(ISO/IEC TR 13066-2:2016) Degree to which a computer system is easy to use by all people, including those with disabilities.

Access control

(ISO/IEC 27000) means to ensure that access to assets is authorized and restricted based on business and security requirements.

Accountability

(ISO/IEC 2382:2015) property that ensures that the actions of an entity may be traced uniquely to that entity.

Acquisition

(ISO/IEC 27037:2012) process of creating a copy of data within a defined set (the product of an acquisition is an evidentially reliable copy of the original source data).

Assurance

(ISA 62443-1-2) Attribute of a system that provides grounds for having confidence that the system operates such that the system security policy is enforced.

Audit

(ISO/IEC 27000:2016) systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled (An audit can be an internal audit or an external audit, and it can be a combined audit).

(ISA 62443-1-2) independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Asymmetric cryptographic algorithm

(ISO/IEC 10181-1:1996, definition 3.3.1) algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ.

Attack

(ISO/IEC 27000:2016) attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Authentication

(ISO/IEC 27000) provision of assurance that a claimed characteristic of an entity is correct.

Availability

(ISO/IEC 27000:2016) property of being accessible and usable upon demand by an authorized entity.

Biometrics

(ISO/TR 18307:2001) use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of entities.

Certification

(Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency") Certification consists of the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance. Certification serves the purpose to inform and reassure purchasers and users about the security properties of the products and services that they buy or use.

Collection

(ISO/IEC 27037:2012) process of gathering the physical items that contain potential digital evidence.

Confidentiality

(ISO/IEC 27000:2016) property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Conformity

(ISO/IEC 27000:2016) fulfilment of a requirement.

Cryptanalysis

(ISO/IEC 7498-2:1989, definition 3.3.18 and ISO/IEC 18033-1 2015) the analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.

Cryptology

(Computer Security – Dieter Gollmann – Johnson Wileys and Sons) Cryptology groups together by definition of Cryptography (i.e. "the science of secret writing") and Cryptanalysis (i.e. the science of "breaking ciphers") . For the scope of this taxonomy, under this domain go not only the mathematical foundations, but also the technical implementations of cryptographic algorithms and architectures, as well as the implementation of cryptanalytic methodologies, techniques and tools.

Cybercrime

(ISO/IEC 27032:2012) criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime.

Cybersecurity

(ISO/IEC 27032:2012) preservation of confidentiality, integrity and availability of information in the Cyberspace.

(the) Cyberspace

(ISO/IEC 27032:2012) complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.

Data

(ISO/IEC 27000:2016) collection of values assigned to base measures, derived measures and/or indicators.

Digital evidence

(ISO/IEC 27037:2012) information or data, stored or transmitted in binary form

that may be relied on as evidence.

Digital signatures

(ISO/IEC 14888) process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature.

Digital Rights Management

(ISO/IEC 5127:2017) digital technology that is separate to the product form of a specific digital publication and which is used to control access to content.

Distributed System

(Coulouris, George; Jean Dollimore; Tim Kindberg; Gordon Blair (2011). Distributed Systems: Concepts and Design (5th Edition). Boston: Addison-Wesley. ISBN 0-132-14301-1) A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages. In this context cybersecurity deals with all the aspects of coordination, message integrity, availability and (if required) confidentiality. Message authentication is also in the scope.

Documented information

(ISO/IEC 27000:2016) information required to be controlled and maintained by an organization and the medium on which it is contained.

eIDAS

(Regulation (EU) No 910/2014) EU regulation proposed to ensure that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available;

Effectiveness

(ISO/IEC 27000:2016) extent to which planned activities are realized and planned results achieved.

Event

(ISO/IEC 27000:2016) occurrence or change of a particular set of circumstances.

Executive management

(ISO/IEC 27000:2016) person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organization.

Governance of information security

(ISO/IEC 27000:2016) system by which an organization’s information security activities are directed and controlled.

Governing body

(ISO/IEC 27000:2016) person or group of people who are accountable for the performance and conformance of the organization.

Hash functions

(ISO/IEC 10118-1:2016) Hash-functions map strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, using a specified algorithm. They can be used for reducing a message to a short imprint for input

to a digital signature mechanism, and committing the user to a given string of bits without revealing this string.

Human errors

Mistakes that unwittingly create opportunities for cyber hackers to exploit.

Identity

(ISO/IEC 24760-1:2011) set of attributes related to an entity.

Identity management

(ISO/IEC 24760-1:2011) processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain.

Indicator

(ISO/IEC 27000:2016) measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs (2.31).

Identification

(ISO/IEC 27037:2012) process involving the search for, recognition and documentation of potential digital evidence.

Information security

(ISO/IEC 27000:2016) preservation of confidentiality, integrity and availability of information.

Information security continuity

(ISO/IEC 27000:2016) processes and procedures for ensuring continued information security operations

Information security event

(ISO/IEC 27000:2016) identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.

Information security incident

(ISO/IEC 27000:2016) single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information security incident management

(ISO/IEC 27000:2016) processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Information system

(ISO/IEC 27000:2016) applications, services, information technology assets, or other information handling components.

Integrity

(ISO/IEC 27000:2016) property of accuracy and completeness.

ISMS project

(ISO/IEC 27000:2016) structured activities undertaken by an organisation (2.57) to implement an ISMS.

Key management

(ISO/IEC 11770-1:2010 PART 1, definition 2.28) administration and use of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy

Level of risk

(ISO/IEC 27000:2016) magnitude of a risk (2.68) expressed in terms of the combination of consequences (2.14) and their likelihood.

Likelihood

(ISO/IEC 27000:2016) chance of something happening.

Malware

(ISO/IEC 27033-1:2015) malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.

Management system

(ISO/IEC 27000:2016) set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.

Message authentication

(ISO/IEC 9797-1) process to authenticate a message, often done through Message authentication codes (string of bits which is the output of a MAC algorithm.

Monitoring

(ISO/IEC 27000:2016) determining the status of a system, a process (2.61) or an activity.

Network security

(ISO/IEC TR 29181-5) Network security is concerned with hardware, software, basic communication protocols, network frame structure, and communication mechanisms factors of the network. Information Security in the network context deals with data integrity, confidentiality, availability and non-repudiation while is sent across the network.

Non-conformity

(ISO/IEC 27000:2016) non-fulfilment of a requirement.

Non-repudiation

(ISO/IEC 27000:2016) ability to prove the occurrence of a claimed event for action and its originating entities.

Organization

(ISO/IEC 27000:2016) person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

Outsource

(ISO/IEC 27000:2016) make an arrangement where an external organization performs part of an organization's function or process.

Performance

(ISO/IEC 27000:2016) measurable result.

Personally Identifiable Information (PII)

(ISO/IEC 24745:2011) any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains; from which identification or contact information of an individual person can be derived, or that is or might be directly or indirectly linked to a natural person.

Policy

(ISO/IEC 27000:2016) intentions and direction of an organization as formally expressed by its top management.

Post-quantum cryptology

(NISTIR 8105) the goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

Preservation

(ISO/IEC 27037:2012) process to maintain and safeguard the integrity and/or original condition of the potential digital evidence.

Process

(ISO/IEC 27000:2016) set of interrelated or interacting activities which transforms inputs into outputs.

Protection Profile

(ISO/IEC 15408-1:2009) implementation-independent statement of security needs for a Target of Evaluation (TOE) type.

Privacy

(ISO/TS 25237:2008) freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.

Privacy Enhancing Technology (PET)

(ISO/IEC 29100:2011) privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system.

Pseudonymity

(ISO/IEC 25237:2017) particular type of de-identification that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms.

Quantum cryptology

(ISO/TS 80004-12:2016(en), 6.6) use of quantum phenomena for cryptographic purposes.

Reliability

(ISO/IEC 27000:2016) property of consistent intended behaviour and results.

Reputation

(ISO/IEC 23006-4:2013) measure of the credibility of or the possibility (e.g., legal) for a user to be a party in a transaction.

Requirement

(ISO/IEC 27000:2016) need or expectation that is stated, generally implied or obligatory.

Residual risk

(ISO/IEC 27000:2016) risk remaining after risk treatment.

Review

(ISO/IEC 27000:2016) activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

Risk

(ISO/IEC 27000:2016) effect of uncertainty on objectives. In the context of information security (2.33) management systems, information security risks can be expressed as effect of uncertainty on information security objectives. Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Risk acceptance

(ISO/IEC 27000:2016) informed decision to take a particular risk.

Risk analysis

(ISO/IEC 27000:2016) process to comprehend the nature of risk and to determine the level of risk.

Risk assessment

(ISO/IEC 27000:2016) overall process of risk identification, risk analysis and risk evaluation.

Risk evaluation

(ISO/IEC 27000:2016) process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk identification

(ISO/IEC 27000:2016) process of finding, recognizing and describing risks.

Risk management

(ISO/IEC 27000:2016) coordinated activities to direct and control an organization with regard to risk.

Risk management process

(ISO/IEC 27000:2016) systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk owner

(ISO/IEC 27000:2016) person or entity with the accountability and authority to manage a risk.

Risk treatment

(ISO/IEC 27000:2016) process to modify risk (eg. avoidance, removal, change, share, retain, mitigation).

Scale

(ISO/IEC 27000:2016) ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped.

Security implementation standard

(ISO/IEC 27000:2016) document specifying authorized ways for realizing security.

Security management policy

(ISO/IEC 28000:2007) overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements.

Security Measurements

(NIST SP800-55) Information security measures are used to facilitate decision making and improve performance and accountability through the collection, analysis and reporting of relevant cybersecurity performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements.

Security Target

(ISO/IEC 15408-1:2009) implementation-dependent statement of security needs for a specific identified Target of Evaluation (TOE).

Symmetric cryptographic algorithm

(ISO/IEC 9735-1, definition 4.111) algorithm employing the same value of key for both enciphering and deciphering or for both authentication and validation.

Threat

(ISO/IEC 27000:2016) potential cause of an unwanted incident, which may result in harm to a system or organization.

Testing

(ISO/IEC 29109-1:2009) determination of one or more characteristics of an object of conformity assessment, according to a procedure.

Top management

(ISO/IEC 27000:2016) person or group of people who directs and controls an organization at the highest level.

Trust

(ISO/IEC 25010:2011) degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

Unlinkability

(ISO/TS 12812-2:2017) security property of a protocol that protect it against an unauthorized party being able to link two executions of the protocol to a specific mobile device.

Validation

(ISO/IEC 27000:2016) confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

Verification

(ISO/IEC 27000:2016) confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

Vetting (referred to employees' recruitment)

(Collins online dictionary) Employees screening.

Vulnerability

(ISO/IEC 27000) weakness of an asset or control that can be exploited by one or more threats.

List of figures

Figure 1. Cybersecurity taxonomy definition steps. 8

Figure 2. Vertical and horizontal cybersecurity development areas 9

Figure 3. ETSI cross-cutting cybersecurity clusters 13

Figure 4. IFIP TC 11 Structure 14

Figure 5. High-level overview of the concepts and vocabularies emerged from the analysis 25

Figure 6. High Level view of the Cybersecurity Taxonomy 27

List of tables

Table 1. European Projects Catalogue dimensions 9
Table 2. ACM Classification System Categories 10
Table 3. Cybersecurity Topic Clustering (NIST Computer Security Resource Center) 11
Table 4. ETSI TC-Cyber working group domains 12
Table 5. IFIP WG 11 Research sub-groups 16
Table 6. List of Standards taken into consideration 17
Table 7. Sources contributions to the Cybersecurity Taxonomy 24

Annex 6: Pilot Project: Work Programme Text and Timeline

Extract from

EN

Annex 6

Horizon 2020

Work Programme 2018-2020

5.i. Information and Communication Technologies

Important notice on the Horizon 2020 Work Programme

This Work Programme covers 2018, 2019 and 2020. The parts that relate to 2019 and 2020 are provided at this stage on an indicative basis. Such Work Programme parts will be decided during 2018 and/or 2019.

(European Commission Decision C(2017)7124 of 27 October 2017)

SU-ICT-03-2018: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap

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

The Public Private Partnership on Cybersecurity[20] created in 2016 was an important first step aiming at triggering up to EUR 1.8 billion of investment. However, the scale of the investment under way in other parts of the world suggests that the EU needs to do more in terms of investment and overcome the fragmentation of capacities spread across the EU. In this context in a recent Joint Communication[21] the Commission announced the intention to create a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.

Scope: The objective of this topic is to scale up existing research for the benefit of the cybersecurity of the Digital Single Market, with solutions that can be marketable. For this, participants should in parallel propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub. Projects under this topic will help build and strengthen cybersecurity capacities across the EU as well as provide valuable input for the future set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre as mentioned by the Joint Communication.

To achieve the above, support will go to consortia of competence centres in cybersecurity to engage together in:

- Common research, development and innovation in next generation industrial and civilian cybersecurity technologies (including dual-use), applications and services; focus should be on horizontal cybersecurity technologies as well as on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing);

[20] C(2016) 440 final

[21] Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN (2017) 450 final

- Strengthening cybersecurity capacities across the EU and closing the cyber skills gap;
- Supporting certification authorities with testing and validation labs equipped with state of the art technologies and expertise.

Each proposal should bring together cybersecurity R&D&I centres in Europe (e.g. university labs/public or private non-profit research centres) to create synergies and scale up existing competences and demonstrated strengths to the European level. Proposals should take into consideration relevant active digital ecosystems and public-private cooperation models and focus on solving technological and industrial challenges. The centres within the proposal should aim to collectively develop and implement a Cybersecurity Roadmap covering the above and addressing multiple and complementary cybersecurity disciplines (e.g. cryptography, network security, application security, IoT/cloud security, data integrity and privacy, secure digital identities, security/crisis management, forensic technologies, security investigation, cyber psychology, bio-security). When developing the Roadmap the results of the work done by the cPPP on cybersecurity, notably its Strategic Research and Innovation Agenda, will serve as a starting point. Consideration should also be given to the relevant work of ENISA, Europol and other EU agencies and bodies.

The Roadmap should include targets to be achieved with deliverables by the end of the project (typically three to four years) that constitute clear milestones in its implementation, as well as priorities to be addressed in the future by the Cybersecurity Competence Network.

To implement this Roadmap, partners in the proposal(s) are expected to set up a functional network of centres of expertise with a coordinating "competence centre" (this role should be undertaken by one of the partners in the network, with the necessary capacity, resources and experience). Work includes the assessment of various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria, including the EU mechanisms and rules, national and regional funding structures, as well as those offered by industry. Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people) and will be implemented, tested and validated in the demonstration cases (see below) involving all partners in the network to showcase (in a measurable manner) its performance and optimise the suggested governance structure.

Projects will demonstrate the effectiveness of their selected governance structure by providing collaborative solutions to enhance cybersecurity capacities of the network and develop cyber skills (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; align cybersecurity certification programmes; classify skills with work roles).

Projects should ensure outreach, to raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, and to spread the developed expertise.

Projects should also include industrial partners and their cybersecurity research collaborators to create synergies and: (a) collaboratively identify and analyse

scalable (short/mid/long term[22]) cybersecurity industrial challenges in the selected sectors and (b) demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through (not less than four) research and innovation demonstration cases.

These demonstration cases will constitute the core part of the work to be done within the project. They will be based on a specific research & development roadmap to tackle selected industrial challenges and will implement it covering a complete range of activities, from research & innovation through testing, experimentation and validation to certification activities.

Projects under this topic are implemented as a programme through the use of complementary grants. The respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement will be applied. Proposals shall therefore foresee resources for clustering activities with other projects funded under this topic to identify synergies, best practices and kick-off the process of creating the network involving the sub-networks already created by awarded projects. This task will contribute to the actual set-up of the Cybersecurity Competence Network and a European Cybersecurity Research and Competence Centre at a later stage.

A proposal must involve distinct cybersecurity R&D&I excellence centres in Europe (e.g. university labs, public or private non-profit research centres, taking into consideration public-private cooperation models and the ecosystems around them), with complementary expertise, from at least 9 Member States or Associated Countries. With the aim of reinforcing technology and industrial capacity as widely as possible across Europe, proposals should include a substantial representation of the most relevant RD&I excellences centres in Europe, with a widespread European coverage and good geographical balance of activities as regards the scope of work. This will ensure the proposals meeting the policy goals of the initiative of supporting the establishment of the future Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre of the European Union.

The consortium in a proposal must involve at least 20 partners.

A proposal should also include industrial partners from various (not less than 3) sectors (e.g. telecom, finance, transport, eGovernment, health, space, defence, manufacturing) that will be involved in the demonstration cases.

The support and involvement of the relevant governmental bodies and authorities (e.g. for monitoring and assessing the projects' results during their life-cycles) will be considered as an asset.

The Commission considers that proposals requesting a contribution of up to EUR 16 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

---

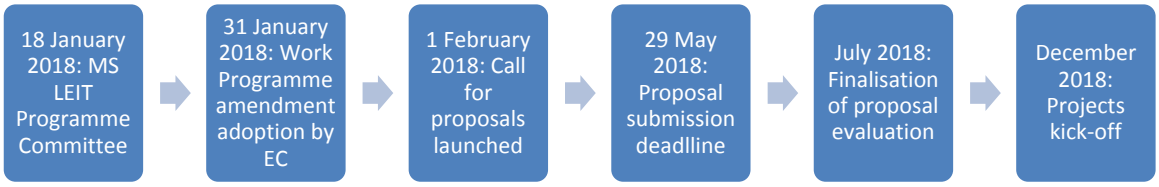
[22] *Short term*: referring to cybersecurity challenges in existing industrial products that can be addressed by the research and computational capabilities of the Network, *medium term*: referring to cybersecurity challenges in upcoming products that can be addressed by the research and computational capabilities of the Network and the Center and *long term*: high risk research for challenges that will shape new policies for long-term innovation capabilities requiring computational and research capacities beyond the existing ones by the Network.

For grants awarded under this topic the Commission may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.

Under this call topic, the beneficiaries nominated as project coordinators cannot, in this capacity, be awarded more than one grant from the European Union budget. In case an applicant organisation appears as coordinator in more than one proposal, only the last submitted proposal will be considered for evaluation. This approach should allow different governance models to be tested through this topic and provide a wide range of complementary outcomes, including lessons learnt, for the future set-up.

Expected Impact:

- Cybersecurity solutions, products or services for the identified critical challenges, increasing the cybersecurity of the Digital Single Market, in particular for sectors from which stakeholders are involved;
- A feasible, sustainable governance model for the Cybersecurity Competence Network developed and tested through successful pilot projects addressing selected industrial challenges;
- Clearly demonstrated strengthening of Member States' research and innovation competence and cybersecurity capacities, also within their national cybersecurity ecosystems, to meet the increasing cybersecurity challenges;
- Synergies between experts from various cybersecurity domains demonstrated;
- Bridges built between the network and industrial communities;
- Research and Development programme with a common Research and Innovation Roadmap reflecting all different cybersecurity sectors and covering a wide range of activities from research to testing;
- A cybersecurity skills framework model developed, which can be used as a reference by education providers to develop appropriate curricula; by employers, to help assess their cybersecurity workforce, and improve job descriptions; by citizens to reskill themselves;
- Establishment of foundations for pooling and streamlining the development and deployment of cybersecurity technology and strengthening industrial capabilities to secure EU's digital economy, society, democracy, space and infrastructures.

Type of Action: Research and Innovation action

1 PILOT PROJECT: TIMELINE