
JRC TECHNICAL REPORTS

# A Proposal for a European Cybersecurity Taxonomy

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

2019

**EU Science Hub**
https://ec.europa.eu/jrc

JRC118089

EUR 29868

PDF ISBN 978-92-76-11603-5 ISSN 1831-9424 doi:10.2760/106002

Luxembourg: Publications Office of the European Union, 2019



How to cite this report: NAI-FOVINO, I., NEISSE, R., HERNANDEZ-RAMOS, J. L., POLEMI, N., RUZZANTE, G., FIGWER, M., LAZARI, A., A Proposal for a European Cybersecurity Taxonomy, EUR 29868, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11603-5, doi:10.2760/106002, JRC118089.

# Contents

## Abstract

The Commission made a commitment in the Communication adopted in September 2018 (COM (2018) 630 final) 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

On 12 September 2018, the Commission has proposed a Regulation setting up a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres (COM/2018/630). The overall mission of the Competence Centre and the Network (CCCN) is to help the Union retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market. This goes hand-in-hand with the key objective to increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other European industries.

One of the first steps during the Impact Assessment of the Proposed Regulation was to provide a clear definition of the cybersecurity context, its domains of application, research and knowledge. In this context, the first version of the proposed taxonomy was published[1] with the goal of aligning the cybersecurity terminologies, definitions and domains. The taxonomy was then used for 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. Based on this first analysis, a survey was also conducted where more than 600 institutions participated and registered their cybersecurity expertise[2].

In order to assess essential aspects of the CCCN regulation proposal, the Commission launched a pilot phase under Horizon 2020. In particular, the proposals CONCORDIA[3], ECHO[4], SPARTA[5] and CyberSec4Europe[6] were selected as the four pilot projects to assist the EU in the establishment of a European Cybersecurity Competence Network of cybersecurity centres of excellence[7]. The pilots bring together more than 160 partners, including big companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States.

The four pilot projects were asked to review the proposed taxonomy and provided feedback, which was used to improve the first version of the taxonomy in order to publish this second enhanced version.

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:

[1] http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf
[2] https://ec.europa.eu/jrc/en/research-topic/cybersecurity/cybersecurity-competence-survey
[3] https://www.concordia-h2020.eu
[4] https://www.echonetwork.eu
[5] https://www.sparta.eu
[6] https://www.cybersec4europe.eu
[7] COM(2018) 630 final

- 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. Section 2.3 summarises the main concepts emerged from the analysis while Section 3 presents in detail the proposed taxonomy. Section 4 presents guidelines on the usage of the taxonomy and Section 5 concludes this report with final remarks. 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.

## 2.1 Methodology

Taxonomy is defined as "*the practice of classification of things or concepts, including the principles that underlie such classification*"[8].

One of things to bear in mind about taxonomies is that there is never one uniquely valid taxonomy for a given domain, but that a 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 deduce:

   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;

(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.

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

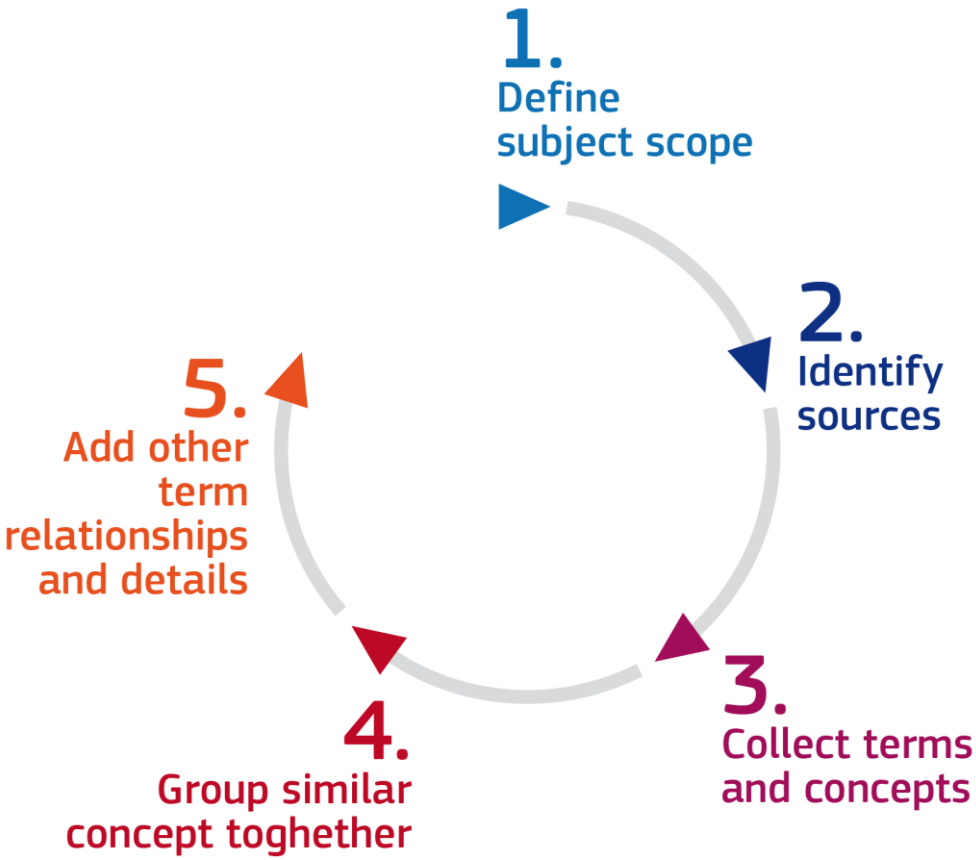


*Figure 1: Cybersecurity taxonomy definition steps.*

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 taxonomies 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)[9] is an initiative falling under the *Coordination and Support Action* scheme aiming at "*defining and promoting a pragmatic approach to implement 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<br>▪ Collaborative platform<br>▪ Cyber security<br>▪ Privacy<br>▪ Big Data | ▪ Digital Health<br>▪ Energy<br>▪ Engineering & manufacturing<br>▪ Finance & insurance<br>▪ ICT<br>▪ Local & public administrations<br>▪ National government agencies<br>▪ 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 activity, and the target applications and technologies.

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

#### *2.2.1.2 ACM Classification System*

The Association for Computing Machinery (ACM) proposed a Computing Classification System (CCS)[10] 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:

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

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

| Software and application security | Systems security |
|---|---|
| ▪ Software security engineering<br>▪ Web application security<br>▪ Social network security and privacy<br>▪ Domain-specific security and privacy architectures<br>▪ Software reverse engineering | ▪ Operating systems security<br>▪ Mobile platform security<br>▪ Trusted computing<br>▪ Virtualization and security<br>▪ Browser security<br>▪ Distributed systems security<br>▪ Information flow control<br>▪ Denial-of-service attacks<br>▪ Firewalls<br>▪ Vulnerability management<br>▪ Penetration testing<br>▪ Vulnerability scanners<br>▪ File system security |

*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)11, 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;
- 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.

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

| 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 appropriate 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[12] 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
- **Cryptography:** Ciphers, Encryption, Public key, Quantum cryptography, Random number generation, Side-channel attacks;
- **Data security:** Cryptography, Message authentication; Digital signatures;

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

- **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[13] 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<br>▪ Security controls<br>▪ Network and Information Security<br>▪ Critical infrastructures<br>▪ Information Security Indicators | ▪ Mobile/Wireless systems (3G/4G, TETRA, DECT, RRS, RFID…)<br>▪ IoT and Machine-to-Machine (M2M)<br>▪ Network Functions Virtualisation<br>▪ Intelligent Transport Systems, Maritime<br>▪ Broadcasting | ▪ Lawful Interception and Retained Data<br>▪ Digital Signatures and trust service providers<br>▪ Secure elements<br>▪ Exchangeable CA/DRM solutions<br>▪ Cryptography |

*Table 4: ETSI TC-Cyber working group domains*

Moreover, ETSI presents an overview of the Global Cyber Security Ecosystem specifying 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 areas of activity, 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 Figure 3).

[13] 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[14] (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[15].

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).

[14] http://ifip.org/
[15] https://www.ifiptc11.org/

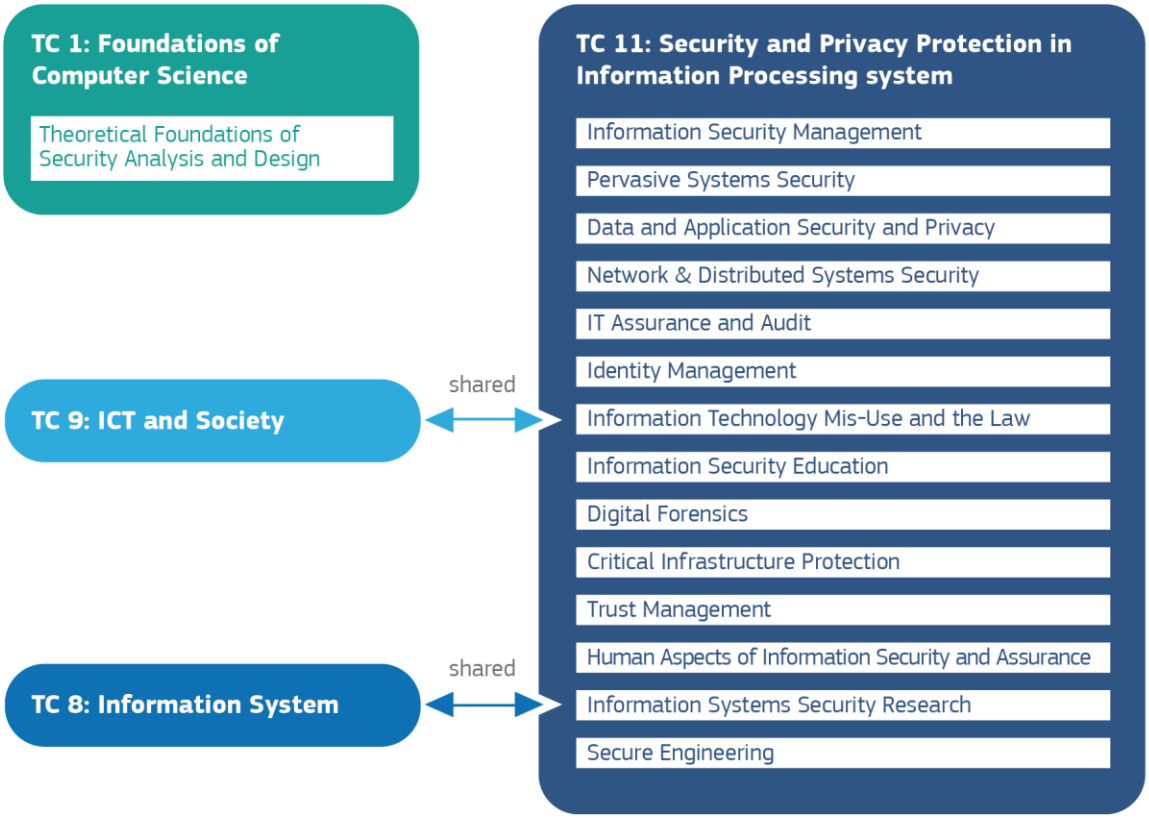


*Figure 4: IFIP TC 11 Structure*

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**<br><br>• Formal definition and verification of the various aspects of security, confidentiality, integrity, authentication and availability;<br>• New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their manifold applications (e.g., electronic commerce);<br>• Information flow modelling and its application to the theory of confidentiality policies, composition of systems, and covert channel analysis;<br>• Formal techniques for the analysis and verification of mobile code;<br>• Formal analysis and design for prevention of Denial of Service (DoS). | **WG 11.1 Information Security Management**<br><br>• Upper management awareness on information security<br>• Managerial aspects concerning information security<br>• Assessment of information security effectiveness and degree of control by managers;<br>• Risk analysis<br>• Identification of threats and vulnerabilities<br>• Measurement and assessment of security levels in a company<br>• Identification of the impact of hardware and software changes on the management of Information Security;<br>• Technical aspects;<br>• Standards for Information Security;<br>• Disaster recovery. | **WG 11.2 Pervasive Systems Security**<br><br>• Information security particularly related to pervasive systems |
| **WG 11.3 Data and Application Security and Privacy**<br>• Statement of security and privacy requirements for data management systems;<br>• Design, implementation, and operation of data management systems that include security and privacy functions;<br>• Assurance that implemented data management systems meet their security and privacy requirements. | **WG 11.4 Network & Distributed Systems Security**<br>• Management and technicians awareness in respect of the reliable and secure operation of the information networks;<br>• Education and training in the application of security principles, methods, and technologies to networking;<br>• Network aspect of information systems security;<br>• Managerial, procedural and technical aspects of network security;<br>• Requirements for network security;<br>• Network oriented cybersecurity risk analysis;<br>• Network security controls | **WG 11.5 IT Assurance and Audit**[16]<br><br>• IT audit in financial statement review;<br>• IT assurance reporting standards;<br>• IT risk management and Enterprise Risk Management (ERM);<br>• Continuous assurance and audit;<br>• Information assurance;<br>• Software assurance;<br>• Governance, Risk and Compliance (GRC);<br>• Service assurance tooling. |
| **WG 11.6 Identity Management**<br><br>• Identity management<br>• Biometric technologies<br>• National identity management | **WG 11.7 / 9.6 Information Technology Misuse and Law**[17]<br>• Analysis of existing and emerging threats to IT systems security, and the associated risks to people, organisations and society.<br>• Analysis of security principles;<br>• Aspects of the law where the use or introduction of IT on a global scale has rendered the current law (and/or its interpretations) obsolete or obsolescent or made it unenforceable;<br>• Analysis of potential means of countering and mitigating threats, e.g. legal frameworks, ethical standards, managerial procedures, and other social factors applicable to behaviour and responsibilities in the context of IT systems;<br>• Possible solutions;<br>• New legal, social and organisational consequences of the development and use of IT systems. | **WG 11.8 IT Security Education**<br><br>• Education and training in information security.<br>• Courses in information security at the university level;<br>• Business educational training on information security modules<br>• Collection, exchange and dissemination of information relating to information security courses conducted by private organizations for industry;<br>• Collection and periodical dissemination of annotated bibliography of information security books, feature articles, reports, and other educational media. |

[16] http://www.ifip.org/bulletin/bulltcs/tc11_aim.htm#wg115
[17] http://www.ifip.org/bulletin/bulltcs/tc9_aim.htm#wg96

| WG 11.9 Digital Forensics | WG 11.10 Critical Infrastructure Protection | WG 11.11 Trust Management |
|---|---|---|
| • Theories, techniques and tools for extracting, analyzing and preserving digital evidence;<br>• Network and cloud forensics;<br>• Embedded device forensics;<br>• Digital forensic processes and workflow models;<br>• Digital forensic case studies;<br>WG 11.9 Digital Forensics<br>• Theories, techniques and tools for extracting, analyzing and preserving digital evidence;<br>• Network and cloud forensics;<br>• Embedded device forensics;<br>• Digital forensic processes and workflow models;<br>• Digital forensic case studies;<br>• Legal, ethical and policy issues related to digital forensics. | • Infrastructure vulnerabilities, threats and risks;<br>• Security challenges, solutions and implementation issues;<br>• Infrastructure sector interdependencies and security implications;<br>• Risk analysis, risk assessment and impact assessment methodologies;<br>• Modeling and simulation of critical infrastructures;<br>• Legal, economic, policy and human factors issues related to critical infrastructure protection;<br>• Secure information sharing;<br>• Infrastructure protection case studies;<br>• Distributed control systems/SCADA security;<br>• Telecommunications network security; | • Semantics and models for security and trust;<br>• Trust management architectures, mechanisms and policies;<br>• Trust in e-commerce, e-service, e-government;<br>• Trust and privacy;<br>• Identity and trust management;<br>• Trust in securing digital as well as physical assets;<br>• 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;<br>• Awareness and education methods;<br>• Enhancing risk perception;<br>• Public understanding of security;<br>• Usable security;<br>• Psychological models of security software usage;<br>• User acceptance of security policies and technologies;<br>• User-friendly authentication methods;<br>• Automating security functionality;<br>• Non-intrusive security;<br>• Assisting security administration;<br>• Impacts of standards, policies, compliance requirements;<br>• Organizational governance for information assurance;<br>• Simplifying risk and threat assessment;<br>• Understanding motivations for misuse;<br>• Social engineering and other human-related risks;<br>• Privacy attitudes and practices;<br>• Computer ethics and security. | • Theoretical and empirical analyzes of information security behaviour;<br>• Adoption, use, and continuance of information security technologies and policies;<br>• Compliance with information security and privacy policies, procedures, and regulations;<br>• Investigations of computer crime and security violations;<br>• Motivators and inhibitors of employee computer crime;<br>• Forensic analysis of security breaches and computer crimes;<br>• Individual, organizational, and group information privacy concerns and behaviors;<br>• Legal, societal, and ethical issues in information security;<br>• investigations of information security behaviour (Neurosecurity). | • Security requirements engineering with emphasis on identity, privacy and trust:<br>• Secure Service Architectures and Design:<br>• Security support in programming environments<br>• Service composition and adaptation:<br>• Risk and Cost-aware Secure Service Development:<br>• Security assurance for services:<br>• 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 80004 |
| ISO/IEC 5127 | ISO/IEC 25010 | ISO/IEC 27033 | ISO/TS 12812-2 |
| ISO/IEC 9735 | ISO/IEC 25237 | ISO/IEC 27035 | ISO/IEC 15408 (Common Criteria) |
| ISO/IEC 10118 | ISO/IEC 27000 | ISO/IEC 27037 | ISA 62443 |
| ISO/IEC 10181 | ISO/IEC 27001 | ISO/IEC 28000 | NIST SP 800, SP 800 55 |
| ISO/IEC 11770 | ISO/IEC 27002 | ISO/IEC 29100 | ETSI:tr (cyber) |
| ISO/IEC 11889 | ISO/IEC 27004 | ISO/IEC 29109-1 | |
| ISO/IEC 18033 | ISO/IEC 27005 | ISO/TR 18307 | |
| ISO/IEC 23006-4 | ISO/IEC 27019 | ISO/TR 11633-2 | |

*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[18].

- *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[19] "Internet Security Glossary, Version 2" produced by the Network Working Group;
    - Intel Threat Agent Library (TAL)[20] and Threat Agent Motivation[21];
    - MACE Taxonomy, Adversary Types[22];
    - CAPEC ATT&CK from Mitre[23];
    - Cyber Kill Chain[24];
- *Tallinn Manual on the International Law Applicable to Cyber Warfare prepared by the NATO Cooperative Cyber Defence Centre of Excellence;*
- *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[25] 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*"[26]
- *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.

[18] 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.
[19] https://tools.ietf.org/html/rfc4949
[20] https://communities.intel.com/docs/DOC-23853
[21] https://lists.oasis-open.org/archives/cti/201607/msg00044/Intel_Corp_Threat_Agent_Motivations_Feb2015.pdf
[22] http://cradpdf.drdc-rddc.gc.ca/PDFS/unc218/p803340_A1b.pdf
[23] https://attack.mitre.org/mobile/index.php/Main_Page
[24] https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html
[25] https://www.owasp.org/index.php/Glossary accessed in November 2017
[26] http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf accessed in November 2017

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[27] 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.
- *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[28] 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.

[27] https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies accessed in November 2017.
[28] http://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf

- The activities of ECSO are organised around 6 working groups:
  - WG1: Standardisation, certification, labelling and supply chain management, which provided an overview of cybersecurity standards and certification schemes[29]
  - 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(2018) 630 final. 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
- REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (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

[29] https://ecs-org.eu/documents/publications/5a31129ea8e97.pdf

- 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.*

## 2.3 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 applicable 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.

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 reports** | x | | x | x | x | | | | | x |
| **ECSO** | x | | | | | x | x | | | |
| **EU Regulations** (see 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*

# 3 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 goal of the taxonomy is not to support the mapping of cybersecurity products, services, or processes including operational activities.

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 **technologies and use cases** where the cybersecurity foundational research results are applied. Technologies and uses cases typically involve multiple sectors.

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 5, depicts, in a graphical way, the proposed three-dimensional taxonomy, based on the following dimensions:

- **Research domains** represent areas of knowledge related to different cybersecurity aspects. Given the multidisciplinary nature of cybersecurity, such domains are intended to cover different areas, including human, legal, ethical and technological aspects.
- **Sectors** are proposed to highlight the need for considering different cybersecurity requirements and challenges (from a human, legal and ethical perspective) in scenarios, such as energy, transport or financial sector.
- **Technologies and Use Cases** represent the technological enablers to enhance the development of the different sectors. They are related to cybersecurity domains covering technological aspects.

The three-dimensional taxonomy can be used as a reference to map cybersecurity competencies, for example, in Figure 5 an entity working on Cryptology in the Energy sector considering Embedded Systems is mapped.

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.

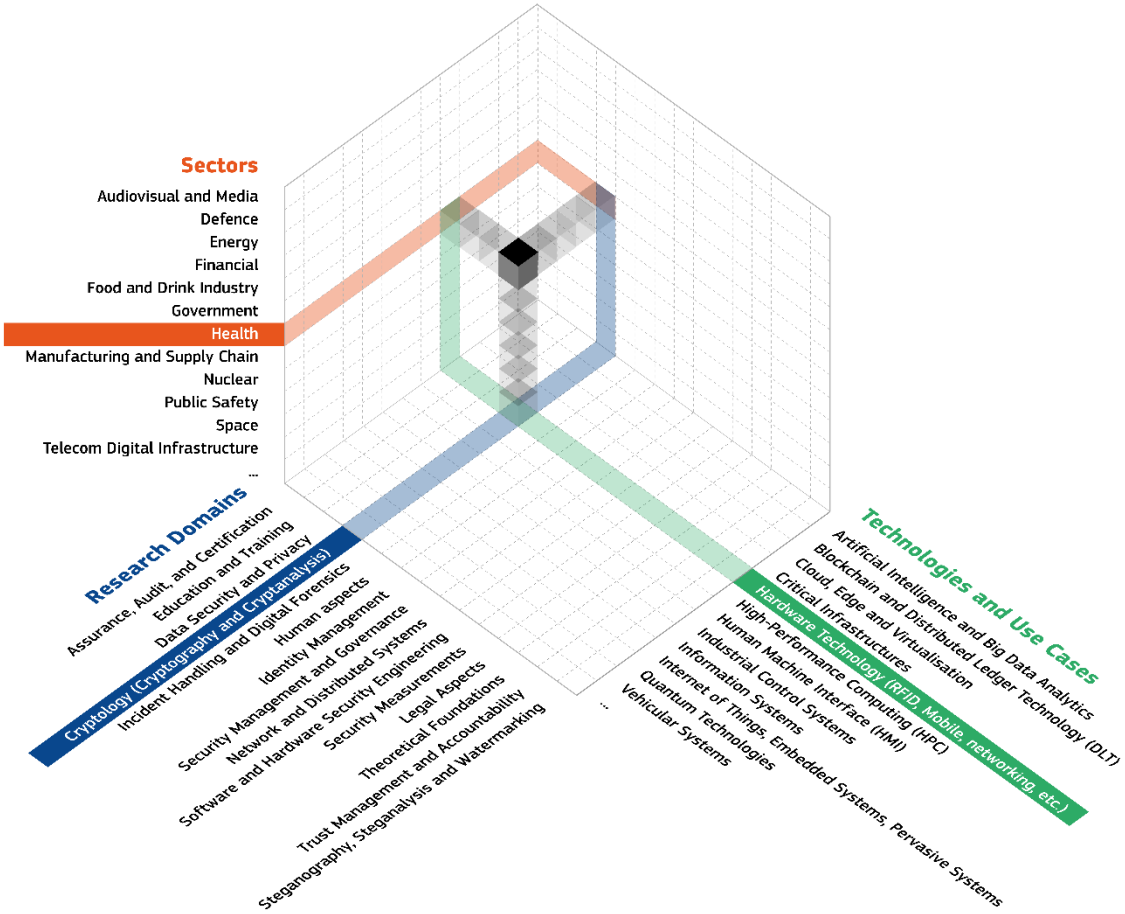


*Figure 5: High Level view of the Cybersecurity Taxonomy*

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 technologies and use cases. The taxonomy is completed with the glossary of concepts and vocabulary included in Annex 1. The cybersecurity subdomains defined for each domain, sectors and technologies/use cases 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, software, service, process 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.

### 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. Furthermore, this domain also considers digital steganography, which is a technique for concealing information in a particular digital format.

- Asymmetric cryptography;
- Symmetric cryptography;
- Cryptanalysis methodologies, techniques and tools;
- Functional encryption;
- Mathematical foundations of cryptography;
- Crypto material management (e.g. key management, PKI);
- Secure multi-party computation;
- Random number generation;
- Digital signatures;
- Hash functions;
- Message authentication;
- Quantum cryptography;
- Post-quantum cryptography;
- Homomorphic encryption.

### 3.1.3 Data Security and Privacy

This domain includes security and privacy issues related to data in order to (a) reduce or avoid by design privacy, confidentiality, and integrity risks without inappropriately 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;
- Anonymity, pseudonymity, unlinkability, undetectability, or unobservability[30];
- Data integrity;
- Privacy Enhancing Technologies (PET);
- Digital Rights Management (DRM);
- Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack);
- Eavesdropping techniques (e.g. via electromagnetic radiation, visual observation of blinking LEDs, acoustic via keyboard typing noise);
- Data usage control.

[30] https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

### 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.

- Higher Education;
- Professional training;
- Cybersecurity-aware culture (e.g. including children education);
- Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness;
- Education methodology;
- Vocational training.

### 3.1.5 Human Aspects

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

- Accessibility;
- Usability;
- Human-related risks/threats (social engineering, insider misuse, etc.)
- Socio-technical security;
- Enhancing risk perception;
- Psychological models and cognitive processes;
- Forensic cyberpsychology;
- User acceptance of security policies and technologies;
- Automating security functionality;
- Non-intrusive security;
- Privacy concerns, behaviours, and practices;
- Computer ethics and security;
- Transparent security;
- Cybersecurity profiling;
- Cyberpsychology;
- Security visualization;
- Gamification;
- Human aspects of trust;
- Human perception of cybersecurity;
- History of cybersecurity.

### 3.1.6 Identity Management

This domain covers processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain. Furthermore, it also considers access management aspects including 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 and attribute management models, frameworks, applications, technologies, and tools (e.g. PKI, RFID, SSO, attribute-based credentials, federated IdM etc.);
- Protocols and frameworks for authentication, authorization, and rights management;
- Privacy and identity management (e.g. privacy-preserving authentication);
- Identity management quality assurance;
- Optical and electronic document security;
- Legal aspects of identity management;
- Biometric methods, technologies and tools.

### 3.1.7 Incident Handling and Digital Forensics

This domain refers to the theories, techniques, tools and processes for the identification, collection, acquisition and preservation of digital evidences.

- Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting;
- Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage);
- Vulnerability analysis and response;
- Digital forensic processes and workflow models;
- Digital forensic case studies;
- Policy issues related to digital forensics;
- Resilience aspects;
- Anti-forensics and malware analytics;
- Citizen cooperation and reporting;
- Coordination and information sharing in the context of cross-border/organizational incidents.

### 3.1.8 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;
- Intellectual property rights;
- Cybersecurity regulation analysis and design;
- Investigations of computer crime (cybercrime) and security violations;
- Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation).

### 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. 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;
- Requirements for 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;
- Network interoperability;
- Secure system interconnection;
- Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication);
- Network steganography.

### 3.1.10 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, including modelling, assessment, analysis and mitigations;
- Modelling of cross-sectoral interdependencies and cascading effects;
- Threats and vulnerabilities modelling;
- Attack modelling, techniques, and countermeasures (e.g. adversary machine learning);
- 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;
- Governance aspects of incident management, disaster recovery, business continuity;

- Techniques to ensure business continuity/disaster recovery;
- Compliance with information security and privacy policies, procedures, and regulations;
- Economic aspects of the cybersecurity ecosystem;
- Privacy impact assessment and risk management;
- Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling);
- Capability maturity models (e.g. assessment of capacities and capabilities).

### 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 visualization;
- Security metrics, key performance indicators, and benchmarks;
- Validation and comparison frameworks for security metrics;
- Measurement and assessment of security levels.

### 3.1.12 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 by 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;
- Security testing and validation;
- Vulnerability discovery and penetration testing;
- Quantitative security for assurance;
- Intrusion detection and honeypots;
- Malware analysis including adversarial learning of malware;
- Model-driven security and domain-specific modelling languages;
- Self-* including self-healing, self-protecting, self-configuration systems;

- Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks);
- Fault injection testing and analysis;
- Cybersecurity and cyber-safety co-engineering;
- Privacy by design.

### 3.1.13 Steganography, Steganalysis and Watermarking

This domain consists of techniques for steganography, steganalysis, and watermarking. Steganography is a technique for hiding secret data within files or message while steganalysis deals with the detection of data hidden using steganography. Digital watermarking is similar to steganography where the embedded data typically is not secret and the goal is also to ensure data integrity.

- Steganography;
- Steganalysis;
- Digital watermarking.

### 3.1.14 Theoretical Foundations

This domain refers to the use analysis and verification techniques based on formal methods to provide theoretical proof of security properties either in software, hardware and algorithm design.

- Formal specification of various aspects of security (e.g properties, threat models, etc.);
- Formal specification, analysis, and verification 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;
- Cybersecurity uncertainty models;
- Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects;

### 3.1.15 Trust Management 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 assess 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 aspects of trust;

- Reputation models;
- Trusted computing;
- Algorithmic auditability and accountability (e.g. explainable AI).

## 3.2 Sectorial Dimensions

The following subsections list sectors proposed for cybersecurity taxonomy.

### 3.2.1 Audiovisual and media

This sector covers traditional media services such as radio, television and cinema but also new media ranging from digital publications to online services including social networks[31].

### 3.2.2 Chemical

This sector covers companies and organizations that produce industrial and consumer chemicals of any sort including petrochemicals, polymers, and basic inorganics.

### 3.2.3 Defence

This sector embraces the activities and infrastructure required for protecting citizens, including the use of aeronautics, space, electronics, land or telecommunication systems[32].

### 3.2.4 Digital Services and Platforms

This sectors includes companies that provide digital services and platforms including cloud services for data storage and web service providers.

### 3.2.5 Energy

This sector includes the companies and organizations intended to produce and distribute energy, including electricity, oil or gas. It comprises the required infrastructure for these activities, such as distribution/storage/transmission system operators, energy production operators, or smart meters and equipment.

### 3.2.6 Financial

This sector embraces the institutions intended to provide financial services, such as banking, insurance or brokerage services.

### 3.2.7 Food and drink

This sector comprises the activities to ensure the production and delivery of safe food/drink and to improve the supply chain. Some of these initiatives include the use of new technological enablers to enhance agriculture and farming activities.

### 3.2.8 Government

This sector refers to the set of systems and activities to implement more efficient governmental services (e.g., eVoting, cybersecurity strategy, public policies, predictions and identification of trends), in order to increase transparency and citizens' participation in political life. It also includes other government services (e.g. border security, fight against crime and terrorism).

[31] https://eurlex.europa.eu/summary/chapter/audiovisual_and_media.html?root_default=SUM_1_CODED%3D05
[32] https://ec.europa.eu/growth/sectors/defence_en

### 3.2.9 Health

This sector includes the companies related to the manufacturing of medical devices (e.g., implantable medical devices), the pharmaceutical industry, as well as the healthcare settings, including hospital and private clinics. It also comprises the activities regarding the monitoring of chronic diseases and elderly people based on the integration of new technologies in the healthcare ecosystem (e.g. smart health).

### 3.2.10 Manufacturing and Supply Chain

This sector includes a vast range of supply chain activities and production techniques, from small-scale enterprises using traditional production techniques, to very large enterprises sitting atop a high and broad pyramid of parts and components suppliers collectively manufacturing complex products[33] (e.g. system or product integration).

### 3.2.11 Nuclear

This sector embraces the set of activities related to nuclear safety, radioactive waste and spent fuel, radiation protection, decommissioning of nuclear facilities, as well as the implementation of safeguards to avoid misuse[34].

### 3.2.12 Safety and Security

This sector represents the set of services related to the protection of citizens and organizations. These services are supported by the corresponding infrastructure intended to prevent and mitigate potential safety-related situations including different use cases such as protection of public spaces, crisis management, and disaster resilience.

### 3.2.13 Space

This sector refers to the set of activities to foster the creation of specific programmes for space exploration. Such programmes space organizations and industry to implement the functionality required to realize such activities, including navigation and time services, Earth observation, or the use of satellite data providers[35].

### 3.2.14 Telecomm Infrastructure

This sector embraces the set of companies and Internet service provides, as well as the infrastructures required to realize such communications (e.g., DNS service providers)

### 3.2.15 Transportation

This sector involves the set of activities related to the movement of humans, animals or objects between two points. This movement can be performed by different means (e.g., air, land or water) and could involve different infrastructure components (e.g., traffic management operators or road authorities), vehicles (e.g., cars, planes or ships) and operations, such as managing and supervise the infrastructure entities.

[33] https://ec.europa.eu/eurostat/statistics-explained/index.php/Manufacturing_statistics_-_NACE_Rev._2
[34] https://ec.europa.eu/energy/en/topics/nuclear-energy
[35] http://ec.europa.eu/growth/sectors/space_en

## 3.3 Technologies and Use Cases Dimension

The following list details, as described at the beginning of this section, the technologies and use cases dimensions. These technologies are used across multiple sectors:

- Artificial intelligence;
- Big Data;
- Blockchain and Distributed Ledger Technology (DLT);
- Cloud, Edge and Virtualisation;
- Critical Infrastructure Protection (CIP);
- Protection of public spaces;
- Disaster resilience and crisis management;
- Fight against crime and terrorism;
- Border and external security;
- Local/wide area observation and surveillance;
- Hardware technology (RFID, chips, sensors, networking, etc.)
- High-performance computing (HPC);
- Human Machine Interface (HMI);e
- Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS);
- Information Systems;
- Internet of Things, embedded systems, pervasive systems;
- Mobile Devices;
- Operating Systems;
- Quantum Technologies (e.g. computing and communication);
- Robotics;
- Satellite systems and applications;
- Vehicular Systems (e.g. autonomous vehicles);
- UAV (unmanned aerial vehicles).

# 4 Guidelines on the Usage of the Taxonomy

The cybersecurity taxonomy described in this report is proposed to support the mapping of entities and their expertise in specific dimensions. As already introduced, this includes the selection of a knowledge domain, sector and technology/use case. In this section, practical guidelines are provided considering issues raised by previous users of the taxonomy.

When selecting the knowledge domains, sectors, technologies and use cases, users of the taxonomy should evaluate how specific or generic is the expertise they are categorizing. Some expertise may be applicable to multiple sectors, technologies and use cases.

In this case, the recommendation is to only specify a knowledge domain and to not select an explicit sector, technology and use case. One example of this could be represented by a user with expertise on formal verification of cryptographic primitives that can be applied to different sectors, as well as technologies and use cases.

The individual association of each knowledge domain with a particular sector, technology and use case may be too cumbersome considering the potential high number of combinations. Therefore, for practical purposes, a common approach is to select each dimension without the specific fine-grained mapping, meaning that the selected knowledge domains apply to all selected sectors, technologies and use cases.

This was the approach adopted in the cybersecurity competence survey conducted using the taxonomy, where for usability reasons the participants simply listed their competences for each dimension without stating their precise matching.

One main issue raised by users is related to the overlap of knowledge domains. For example, the knowledge subdomain of network security in some cases also includes knowledge of cryptography and identity and access management (IAM) approaches.

From a practical perspective, the recommendation in this case is to consider the focus of the research community the entity is part of, and only select the network security subdomain. However, if the user of the taxonomy strongly believes their research contributions on cryptography are self-standing independently of their application on network security, the corresponding subdomain in cryptology should be also selected.

The goal in future refinements of the taxonomy is to evolve in an ontology where the relation between (sub)domains is explicitly defined, so users are informed and guided about the possible overlaps in the classification.

Other concern of taxonomy users is related to domains that could be specialized considering other specific (sub)domains, for example, education focusing on cryptology, legal aspects of identity management, human aspects of privacy, etc.

The recommendation in this case is to focus on the core knowledge domain, for example, in legal aspects of identity management only legal aspects domain should be selected. However, if a fine level of detail is needed, users may select both knowledge domains.

# 5 Final Remarks

The transition of our society toward a cyber-physical reality where physical and digital services are part of the daily life of the citizen is today a fact. However, the way in which digital technologies are intertwined with our lives generates a vicious circle where the more our society becomes digital, the higher is the potential impact of cyber-attacks.

In this context, cybersecurity represents the counterweight of this complex equation, it is the factor allowing the digital revolution to definitively take-off, while preserving the security of citizens' life and well-being. For this reason, cybersecurity occupies today and will continue to occupy even more in the future a relevant position in the development of the European digital society.

The assessment of the European posture towards cybersecurity and the identification of strategies to properly improve cybersecurity in Europe is not trivial. This assessment is important to ensure the development of an adequate level of technology and knowledge autonomy. In this direction, the first step is to answer the key question: "what is cybersecurity?".

The goal of this document is to align the cybersecurity terminologies, definitions and domains to capture, in a systematic manner, all the aspects that together concur in building the cybersecurity realm of knowledge.

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

The resulting three-dimensional taxonomy presented in Section 3 will initially be used to categorise existing EU cybersecurity competence centres (e.g., research organisations, laboratories, associations, academic institutions, groups, operational centres) according to their cybersecurity expertise in specific domains. This categorization aims to support the development of the network of European cybersecurity research and competence centres and will also be the core of the future European Cybersecurity Atlas.

The three-dimensional nature of the taxonomy is extremely flexible, and could also be used in the future to classify and analyse European projects, policy initiatives and beyond.

As a final remark, it is important to keep in mind that cybersecurity is a moving and evolving target. For this reason, this taxonomy cannot be a static entity, 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.

### Adversarial machine learning
(Kurakin, A., Goodfellow, I., & Bengio, S. (2016) Adversarial machine learning at scale. arXiv preprint arXiv:1611.01236) a technique based on the use of adversarial examples, which represent malicious inputs designed to fool machine learning models

### Anonymity
(ISO/IEC 15408) Ensures that a user may use a resource or service without disclosing the user's identity.

### Anti-forensics
(Draft NIST 8006) A set of techniques used specifically to prevent or mislead forensic analysis

### Asymmetric cryptographic technique
(ISO/IEC 9798-5: 2009-12-15 - 3rd ed.) Cryptographic technique that uses two related operations: a public operation defined by a public data item, and a private operation defined by a private data item (the two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation)

### 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.

### 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.

### Awareness
(NIST SP 800-16) A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure.

### 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.

### Business Continuity Plan
(CNSSI 4009-2015) The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

### Capability Maturity Model
(Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993) Capability maturity model, version 1.1. IEEE software, 10(4), 18-27) it is the foundation for systematically building a set of tools, including a maturity questionnaire, which are useful in software process improvement.

### Cascading (Cross Domain)
(CNSSI 4009-2015) The downward flow of information through a range of security levels greater than the accreditation range of a system, network, or component without passing through an isolated device that implements the enforcement of all applicable approved policy decisions for each domain transfer.

### Certification
(ISO/IEC 21827: 2008-10-15 (2nd ed.)) Process, producing written results, of performing a comprehensive evaluation of security features and other safeguards of a system to establish the extent to which the design and implementation meet a set of specified security requirements

### 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.

### Continuous monitoring
(NIST SP 800-150) Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

### Critical Information Infrastructures (CII)
(OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35]) Interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy

### 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.

### Cyber attack
(CNSSI-4009) An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment / infrastructure; or destroying the integrity of the data or stealing controlled information.

### 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.

### 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 forensics
(NIST SP 800-86) The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

### 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.

### Disaster Recovery Plan
(NIST SP 800-82 Rev. 2) A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

### 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.

### Eavesdropping attack
(NIST SP 800-63) An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant.

### Ethics
(ENISA overview of cybersecurity and related terminology - 2017) Are principles and or standards of human conduct. Cyber ethics is a code of behaviour on the Internet. Cyber ethics is the philosophic study of ethics pertaining to computers, encompassing user behaviour and what computers are programmed to do, and how this affects individuals and society

### Fault
(ISO 10303-226) Abnormal condition or defect at the component, equipment, or sub-system level which may lead to a failure.

### Fault Injection Testing
(NIST SP 800-163) Attempting to artificially cause an error with an app during execution by forcing it to experience corrupt data or corrupt internal states to see how robust it is against these simulated failures.

### Fault Tolerant
(NIST SP 800-82 Rev. 2) Of a system, having the built-in capability to provide continued, correct execution of its assigned function in the presence of a hardware and/or software fault.

### Functional encryption
(Boneh, D., Sahai, A., & Waters, B. (2011, March). Functional encryption: Definitions and challenges. In Theory of Cryptography Conference (pp. 253-273). Springer, Berlin, Heidelberg) It is a type of encryption that supports restricted secret keys enabling a key holder to learn a specifi c function of encrypted data, but learn nothing else about the data

### Gamification
(Robson, K., Plangger, K., Kietzmann, J. H., McCarthy, I., & Pitt, L. (2015). Is it all a game? Understanding the principles of gamification. *Business Horizons*, *58*(4), 411-420) The application of game-design elements and game principles in non-game contexts

### 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.

### Homomorphic encryption
(ISO/IEC 18033-6:2019) It is a type of symmetric or asymmetric encryption that allows third parties (i.e. parties that are neither the encryptor nor the decryptor) to perform operations on plaintext data while keeping the data in encrypted form.

### 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.

### Integrity
(ISO/IEC 27000:2016) Property of accuracy and completeness.

### Intrusion Detection
(CNSSI 4009-2015) The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.

### IT Security Metrics
(NIST SP 800-55) Metrics based on IT security performance goals and objectives

### 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

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

### 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.

### Penetration Testing
(NIST SP 800-160) A test methodology intended to circumvent the security function of a system. Note: Penetration testing may leverage system documentation (e.g., system design, source code, manuals) and is conducted within specific constraints. Some penetration test methods use brute force techniques.

### 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.

### 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.

### 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 by design
(Cavoukian, A. (2009) privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada, 5) It is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

### 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.

### Profiling
(CNSSI 4009-2015) Measuring the characteristics of expected activity so that changes to it can be more easily identified.

### 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.

### Public Key Infrastructure (PKI)
(NIST SP 800-53 Rev.4) The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.

### Quality Assurance/Quality Control
(NIST SP 800-160) Part of quality management focused on providing confidence that quality requirements will be fulfilled.

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

### Random Number Generator – (RNG)
(CNSSI-4009) A process used to generate an unpredictable series of numbers. Each individual value is called random if each of the values in the total population of values has an equal probability of being selected.

### Re-identification
(NISTIR 8053) General term for any process that re-establishes the relationship between identifying data and a data subject

### 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.

### Resilience
(NIST SP 800-53 Rev. 4) The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

### 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 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.

### Secure Multiparty Computation
(Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014) e*ncyclopedia of cryptography and security*. Springer Science & Business Media) It refers to cryptographic protocols that allow for the distributed computation of a function over distributed inputs without revealing additional information about the inputs.

### 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.

### Social Engineering
(NIST SP 800-63-2) The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust.

### Steganalysis
It is the study of detecting messages hidden using steganography

### Steganography
(CNSSI 4009-2015) The art, science, and practice of communicating in a way that hides the existence of the communication.

### Symmetric cryptographic technique
(ISO/IEC 9798-1: 2010-07-01 (3rd ed.)) Cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation

### 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.

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

### Trusted Computing
(Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014) e*ncyclopedia of cryptography and security*. Springer Science & Business Media) The belief that a computer will operate in a predictable manner, and provide an environment where data (software and information) within the system is authenticated and protected.

### Unlinkability
(ISO/IEC 15408) Ensures that a user may make multiple uses of resources or services without others being able to link these uses together.

### Unobservability
(ISO/IEC 15408) Ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

### Usability
(NISTIR 8040) The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

### 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.

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

### Vulnerability Analysis/Assessment
(NIST SP 800-53A) Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

### Watermarking
(Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014). *Encyclopedia of cryptography and security*. Springer Science & Business Media) A method in computer security by which identifiers of sources or *copyright owners* of digital or analog signals are embedded into the respective signals themselves in order to keep track of where a signal comes from or who the copyright owners are.

## List of figures

KJ-NA-29868-EN-N

## The European Commission's science and knowledge service

Joint Research Centre

### JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

**EU Science Hub**

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

doi:10.2760/106002

ISBN 978-92-76-11603-5