Kalogeraki *et al. J Surveill Secur Saf* 2024;5:95-115
DOI: 10.20517/jsss.2023.50

Journal of Surveillance, Security and Safety

Original Article

Open Access

Check for updates

A taxonomy for cybersecurity standards

Eleni-Maria Kalogeraki[1,2], **Nineta Polemi**[1,3]

[1]Department of Informatics, University of Piraeus, Piraeus 18534, Greece.
[2]Security Labs Consulting Limited, Cork T12 W7CV, Ireland.
[3]Trustilio B.V., Amsterdam 1017HL, The Netherlands.

Correspondence to: Eleni-Maria Kalogeraki, Department of Informatics, University of Piraeus, Karaoli & Dimitriou str. 80, Piraeus 18534, Greece. E-mail: elmaklg@unipi.gr

How to cite this article: Kalogeraki EM, Polemi N. A taxonomy for cybersecurity standards. *J Surveill Secur Saf* 2024;5:95-115. https://dx.doi.org/10.20517/jsss.2023.50

Received: 11 Dec 2023 **First Decision:** 7 Mar 2024 **Revised:** 8 Apr 2024 **Accepted:** 19 Apr 2024 **Published:** 28 Apr 2024

Academic Editor: Shujun Li **Copy Editor:** Yanbing Bai **Production Editor:** Yanbing Bai

Abstract

Cybersecurity standards on a global scale are exhaustive, appealing to several types, such as glossaries, guidelines, methods, and objectives (e.g., Information Technology evaluation, requirement identification, risk management, and technical specifications). This chaotic range of standards towards the rapid pace of technological and threat evolution hinders stakeholders (e.g., security architects/developers, policymakers, testers, and auditors) from discovering which standards best meet their security needs. The paper analyzes this challenge and contributes to harmonizing standards by identifying relationships between the EU regulation and prominent cybersecurity standards. The current work develops a taxonomy that classifies cybersecurity standards according to their objective, usage, and sector, aiming to help stakeholders understand their purpose and decide which they should adopt to cover their organizational needs. The taxonomy is represented in a semantic ontology, following the Web Ontology Language Edition 2 knowledge engineering approach. A realistic scenario is described to illustrate the applicability of the taxonomy.

Keywords: Cybersecurity standards taxonomy, semantic ontology, AI security, cybersecurity standards classification

INTRODUCTION

Within the last decades, business processes and services have been operating by digitally connected

Information and Communication Technology (ICT) products, engaging several security vulnerabilities and weaknesses. In this light, security requirements across organizations are getting increasingly demanding to cope with the adversaries' gradually improving capacity of launching sophisticated attacks (e.g., botnet DDoS attacks[1], locker ransomware, or crypto-ransomware intrusions[2]) on cyber-physical interdependent systems due to their advanced skills and online access to available sources (e.g., Next-Generation malware toolkits via the Deep/Dark Web employing advance techniques, such as obfuscated memory malware obscuring its presence in the device memory and hiding code scrambling/injection, evade detection activities, *etc*.). Coordinated cyber intrusions, such as RapperBot bruteforce attacks, infected many Internet of Things (IoT) devices using over 3,500 unique IPs worldwide, underpinning the importance of ensuring the security of digital devices)[1]. Another example is the COVID-19-related cyberattacks in Healthcare, which generate data breaches and expose sensitive patient data[3]. The hack of Uganda's largest mobile money networks resulted in a four-day disruption of service transactions, causing a catastrophe in the country's telecom and banking sectors[3]. In this vein, developing new security standards, good practices, and guidelines is a continuous effort to address the diverse security requirements of different organizations, sectors, services, and supply chain operations and guide businesses in raising the security preparedness and resilience of their infrastructures towards the evolving threat landscape.

The landscape of cybersecurity standards seems chaotic due to its complexity and the rapid pace of technological and threat evolution. This perceived chaos stems from several factors:

Plethora of Standardization Bodies: There are numerous cybersecurity standards, frameworks, and guidelines, each developed by different organizations, governments, and industry groups. These include the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), National Institute of Standards and Technology (NIST), European Telecommunications Standards Institute (ETSI), European Committee for Standardization/European Committee for Electrotechnical Standardization (CEN/CENELEC), and sector-specific bodies, such as Health Insurance Portability and Accountability Act (HIPAA) from healthcare, Financial Stability, Financial Services and Capital Markets Union (FISMA) from finance and International Maritime Organization (IMO), Baltic and International Maritime Council (BIMCO) from the maritime sector. The variety can be overwhelming, especially for organizations operating internationally or across multiple sectors.

Rapid Technological Change: The speed at which technology evolves, including the development of cloud computing, IoT devices, artificial intelligence (AI), and quantum computing, challenges existing cybersecurity standards. New technologies often outpace the development and implementation of appropriate security measures.

Evolving Threat Landscape: Cybersecurity threats are constantly changing, with cybercriminals developing new tactics, techniques, and procedures. Standards must adapt to address emerging threats, requiring frequent updates and revisions, which can add to the sense of disorder.

Compliance Complexity: Organizations often find themselves needing to comply with multiple standards simultaneously, which can be costly and resource-intensive. The effort to meet varying requirements can lead to confusion and the perception of chaos, especially when standards overlap or contradict each other.

Industry-Specific Needs: Different industries face unique cybersecurity challenges, leading to the development of industry-specific standards. While necessary, this specialization further fragments the cybersecurity standards landscape.

Cybersecurity management standards, for instance, are developed by all the abovementioned standardization bodies adopting different views; the list of these standards is globally exhaustive, appealing to several types (e.g., glossaries, recommendations, guidelines, methodologies, and metrics) and various topics [e.g., Information Technology (IT) evaluation, security requirement identification, sectorial needs, risk management, and technical specifications]. This chaotic range of standards hinders stakeholders (e.g., policymakers, developers, security architects, integrators, auditors, testers, and risk assessors) of different sectors from deciding which standards to adopt to capture their specific needs.

The implementation of various EU policies and directives (e.g., the Cybersecurity Act[4]) enforces Europe to accelerate its efforts in developing and adopting European standards[5]. Nonetheless, harmonized security standards can provide a technical basis to assess the security of ICT processes/products/services and thus benefit the EU Digital Single Market (DSM) and international digital markets. To this aim, the EU asked the European standardization organizations (e.g., ETSI, CEN/CENELEC) to assess the existing standards and conduct a gap analysis to implement its decision for harmonizing standards (CEN/CENELEC 2023: https://www.cencenelec.eu/media/CEN-CENELEC/News/Publications/2023/workprog2023.pdf). In this paper, we address the need for classifying cybersecurity standards into thematic groups, which can help stakeholders comprehend deeply their content and purpose and facilitate their decision-making upon selecting the most appropriate one to meet their security requirements. Research efforts addressing these topics attract the interest of EU and global industries. European Union Agency for Cybersecurity (ENISA) has recently published an analysis of requirements for standardization in support of cybersecurity policy[6], which serves as a risk management catalog rather than a taxonomy to address published standards of different aspects of risk management and subsequently describe methodologies and tools utilized to conform with or implement these standards. In addition, ENISA has published a framework on distinct cybersecurity skills[7]. The Joint Research Center (JRC) of the European Commission has issued a sectorial categorization covering multiple domains, considered as input in our work to develop a cybersecurity taxonomy based on industry interest[8].

This paper aims to enhance the above work by presenting a taxonomy of prominent cybersecurity management international standards, best practices, and guidelines, articulating them into conceptual groups of different security topics of interest. The current work intends to:

- Contribute to the harmonization of standards efforts by identifying relationships between EU regulation and prominent cybersecurity standards

- Help supply chain operators, industry stakeholders, entrepreneurs, and other interested parties (e.g., security practitioners) to understand the purpose and use of existing cybersecurity standards by classifying them into thematic groups and guiding these entities to select the most appropriate(s) to adopt compared to their needs

- Aid government and business organizations to assess their security policy and best practices

- Provide a robust foundation for the cybersecurity standards taxonomy through the development of a semantic ontology

- Contribute to the cybersecurity standardization work of EU delegates, such as JRC and ENISA

The remainder of the paper is structured as follows: the Related Work section highlights the importance of cybersecurity standardization, provides a picturesque of prominent security standards addressing EU legislation and stresses the need for standards classification. The Taxonomy Building Blocks section presents and analyzes the proposed taxonomy of cybersecurity standards and its ontology structure. The Taxonomy Application section describes the application of the proposed taxonomy under the scope of a focused scenario. Eventually, the last section draws the conclusions from the current work.

RELATED WORK

This section presents work related to security standardization and classification and recognizes gaps. It discusses the priority of cybersecurity standardization in policymaking, describes standards as building blocks of EU security policies, and identifies an interplay of EU legislation with European and international standards.

Cybersecurity as standardization priority in policymaking

A standard is a technical document used as a rule, guideline, or definition. Standards are developed from a group of interested parties (i.e., manufacturers, consumers, and regulators of particular material/products/processes/services) and provide a consensus-built, repeatable dimension[9]. *European Standards (EN)* are implemented by ETSI[10], the national CEN and CENELEC[11].

Cybersecurity is considered a high standardization priority since cyber threats affect multiple sectors. Cybersecurity and data protection are rapidly growing, changing technical and application domains.

The threats and requirements are increasing dramatically with the progress of digitalization and the rising number of critical assets digitalized and accessible online. Within the last decades, the exponential evolution of digital technology among heterogeneous infrastructures of dispersed nodes[12] and the COVID-19 disease has raised the investment in distance work and digital communication. Geopolitical changes and the Ukrainian war increased cyberattacks, whereas the potential of personal data leaks threatens the global digital economy. Internet of Everything (IoE)[13], the networked connection of people, processes, data, and things via the Internet, is the norm for complete digitalization. The requirements of the global ecosystem gradually increase, promoting accelerated productivity to smart objects, such as wearable devices, sophisticated sensor networks and 5G-connected semi-autonomous or autonomous agents, raising the investment in machine-to-machine communication[14].

In the new digital era, the application of emerging technologies, such as augmented reality, global AI, Adversarial Learning, *etc.*, in our daily businesses and the use of digital identity[14] by citizens requires specific practices and guidance on how to manage and monitor and concurrently maintain the security within organizations. The work in[15] stresses the need to boost standardization initiatives and policymaking associated with AI security. More standards for securing AI, 5G and IoT are gradually developed by prominent standardization bodies, addressing various aspects at different levels, with overlaps and diverging approaches[16].

The interplay of EU legislation and international standardization

Security policies in Europe drive us to use and develop standards. For instance, the NIS Directive on Security of Network and Information Systems[17], the most important EU legislation instrument, requires assessing and managing cyber risks among interconnected Critical Infrastructures (CIs). The Critical Entities Resilience Directive (CER)[18] and the proposed Cybersecurity Resilience Act (CRA)[19] stress the need for CI protection and introduce common cybersecurity requirements to apply throughout the

expected lifecycle of devices, respectively. ETSI TR 103 866 V1.1.1[20] and indicative families of standards, i.e., ISO2700x and ISO2800x series, can guide stakeholders to raise compliance with such directives. CEN and CENELEC have introduced numerous sector-specific cybersecurity standards to stress the CI security requirements of critical EU industries[21]. Consequently, security standardization brings trustworthiness to ICT products, spreads knowledge among multiple stakeholders, increases CI protection, and secures digital services.

Cybersecurity certification efforts are accelerating in Europe[22-23] due to the Cybersecurity Act[4], the EU legislation which promotes the certification of EU ICT products, services and processes, addressed by the ENISA Candidate Cybersecurity Certification Scheme (EUCC)[24] and the recent EU implementing act[25], and two additional ENISA cybersecurity certification schemes, i.e., European Cloud Certification Scheme (EUCS) generic cloud scheme[26] and European cybersecurity certification scheme for 5G networks (EU5G)[27]. The EU Cybersecurity Act (EUCSA) relies on international standards for ICT evaluation and conformity assessment[28-30]. Furthermore, cybersecurity certification addresses market fragmentation, increases security, and strengthens the confidence of stakeholders to establish a competitive and resilient EU DSM. ISO and IEC are working on creating a Universal Cybersecurity Labelling Framework [ISO/IEC 27404 (https://www.iso.org/standard/80138.html)], aiming to guide the development and implementation of IoT certification. This involvement is crucial for aligning this new standard with already established IoT security standards, such as ETSI EN 303 645[31] and NISTIR 8425[32] guidance, the primary works for most IoT device specifications worldwide.

Nonetheless, security policies are highly interrelated within the EU. For instance, the EUCSA sets the need for privacy and data protection regulation[33] and for electronic transactions protection in the internal market (eIDAS Regulation)[34]. Privacy and data protection, promoted by General Data Protection Regulation (GDPR)[33], is enhanced to resolve specific matters on natural and legal person rights in the provision and use of electronic communications services by the European ePrivacy Regulation[35]. In this context, privacy-by-design specifications, privacy assessment and management standards are required, such as EN 17529:2022[36], ISO 3300x series on process assessment[37], ISO/IEC 2700x family of standards, and CEN ISO/IEC/TS 27006-2:2022[38], ISO/IEC 27701:2014[39] on privacy information management. The proposed European Data Act[40], which complements the Data Governance Act[41] (i.e., a key pillar of the EU strategy of data), developed to define measures, rules and mechanisms related to industrial data and their accessibility, starts getting into force.

The EUCSA emphasizes the requirement of securing the growing EU markets of the chip industry (i.e., automated cars, cloud and IoT connectivity, space, defense and supercomputers). Chips assumed strategic assets playing a critical role in ICT supply chains. To leverage technological leadership, the EU has started preparing the European Chips Act[42]. In this vein, CEN CENELEC initiates a working group to strengthen the microchip standardization effort in the EU[43].

Eventually, the EUCSA highlights the importance of analyzing emerging technologies. To this aim, the European Artificial Intelligence Act[44] regulation proposal is prepared to secure AI-based systems within the EU borders. CEN CENELEC, upon the request of the European Commission, has established the Joint Technical Committee 21 to produce standardization deliverables on AI[45], whereas ENISA is working on an AI cybersecurity certification scheme[46].

To improve the preparedness, detection, and response to large-scale cybersecurity incidents across the EU, the European Commission proposed the EU Cyber Solidarity Act[47], applied using international standards

on incident management, such as ISO/IEC 27035[48] and NIST recommendations for incident handling[49].

All these EU regulations correspond to the EU Cybersecurity Strategy aiming to "build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies"[50]. Table 1 presents direct or indirect relations between indicative EU legislative instruments and corresponding international or European standards.

The need for cybersecurity standardization classification

Over the past three decades, ICT standards have risen exponentially by a non-stop standards-making ecosystem. The effort of ETSI to enumerate standards venues associated with the proposed EU CRA[19] identified more than 750 of them, originating from different ICT communities of various types of institutional arrangements, technologies, services and working groups[51].

The JRC Technical Report (TR)[8] describes cybersecurity as an interdisciplinary domain engaging a wide use of its application to all industry sectors, embracing different sizes and types of enterprises [e.g., small and medium-sized enterprises (SMEs)/medium-sized enterprises (MEs) and large enterprises], various dimensions (e.g., cyber/physical) utilizing multiple sources addressing some of the most widely-accepted standards, international working groups and classification systems.

This standardization priority of cybersecurity drove the development of several Standard Development Organizations (SDOs), often overlapping in terms of interests and goals and may even, occasionally, act as competitors, which may lead to inconsistencies and redundant requirements that may be confusing to businesses and hurdle their effective use[52].

The list of security standards is wide-ranging and exhaustive, hindering stakeholders from determining which standards can cover their organizational needs. The great variety of standards, recommendations and best practices hinders identifying their interrelations, which would facilitate their understanding.

Considering all these drawbacks of the chaotic list of similar, different, or overlapping security standards, there is a compelling need for their classification into conceptual groups that could better communicate their existence and use to stakeholders.

ETSI standardization body has identified basic principles and practices for ICT standardization and provided a classification of the different types of standardization documents regarding their scope and addressed stakeholders, examining whether they provide requirements or recommendations (normative documents) or communicate relevant information, followed by all SDOs[52]. Moreover, the International Classification for Standards[53] classifies international, regional, and national technical standards and other normative documents designed to map standards in general with every economic sector and virtual activity of humankind used. Notwithstanding, the classification does not address specific aspects of security.

Few attempts to further conceptualize standards have been published already. ENISA has provided a risk management standards framework that analyzes standardization requirements in support of cybersecurity policy and outlines gaps in the domain[6]. The risk management library can guide stakeholders in applying them in their organizations without providing a taxonomy. JRC TR on European Cybersecurity Centers of Expertise Map[8] provides a high-level classification and set of definitions of widely-known standards, international working group classification systems, regulations, best practices, and recommendations in the cybersecurity domain. Nevertheless, the work does not address relations with cybersecurity skills of

Table 1. Security Standards association with EU Regulation

EU Regulation	Standard/Framework/ Best Practices
NIS 2 Directive, CER Directive, CRA Directive (including sector-specific Radio Equipment regulation)	CIs and Risk Assessment: ISO2700x, ISO/IEC 27033, ISO2800x, ETSI TR 103 866 V1.1., ISO/IEC 15408, ISO/IEC 18045, EN 17640, ISO 31000, IACS Recommendation on Cyber Resilience (2020), ANSI/ISA-62443-3-2-2020, ISA-TR99.00.01-2007, Supply chain cybersecurity: new guidance from the NCSC, ISO 13053, ETSI TS 102 165-1:2017, NIST SP-800-53 Cybersecurity Framework, NIST SP-800-37 Risk Management Framework, NIST SP-800-161, ETSI TS 102 165-1, BSI-Standards 100-2/100-3, OWASP Risk, NISTIR 8276 Key-Practices in Cyber Supply Chain Risk Management, NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management, CVRF, ISA/IEC 62443-3-2, IWA 31:2020, ISO 22301, ISO/IEC 27035 Threat taxonomies: OWASP, CAPEC MITRE, FISMA, STRIDE, ATT&CK MITRE Vulnerabilities disclosure: ISO/IEC 29147:2018, EN-ISO/IEC 29147:2020, ISO/IEC 30111:2019, EN-ISO/IEC 30111:2020, TR 103838, CVE (MITRE), CVSS 3.1 (FIRST), OSV
Cybersecurity Act	ENISA: EUCC, EUCS IT Evaluation: ISO/IEC 15408, ISO/IEC 18045, Conformity Assessment/Audit: ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 17000, ISO/IEC 17007, ISO/IEC 17021series, ISO/IEC 17019, ISO/IEC 17020, ISO/IEC 17024, ISO/IEC 17025, ISO/IEC 17065, ISO/IEC 17067, ISO 19011 EU 5G scheme: 3GPP TR 33.894 V0.5.0 (2023-02), ISO/IEC 27404, ETSI EN 303 645, NISTIR 8425 GSMA Network Equipment scheme (Security Assurance-by-design)
GDPR, ePrivacy Regulation, Data Act, eIDAS (including sector-specific EU Health Data Space regulation)	Privacy Assessment/Information Management: EN17529:2022, ISO 3300x series on process assessment, ISO/IEC 2700x information security series, CEN ISO/IEC/TS, 27006-2:2022, ISO/IEC 27701, ISO/IEC TR 27550:2019, BS10012, CEN CWA 16113 Identity Management: ISO/IEC 23220, ISO/IEC 27460, ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 27701, ISO/IEC 27018 Encryption: ISO/IEC 18033, ISO/IEC 11770-3, ISO 13491, ISO/IEC 19772:2020, ISO/IEC 18033-6:2019, ISO 13492:2019
AI Act	EU AI cybersecurity certification scheme proposal, ISO/IEC TR 5469, IEC TS 62998-3, Stocktaking National and Regional Cybersecurity Policy (2021), NIST AI 100-2e2023ipd-Adversarial Machine Learning, ISO/IEC 27005, ISO/IEC 27563, ISO/IEC 23894, ISO/IEC 24028, ISO/IEC 5338
Cyber Solidarity Act	Incident Management: ISO/IEC 27035, NIST Incident Response Framework, NIST SP-800-62 Emergency Management: ISO 22322:2015, ISO 22327:2018, ISO 22326:2018 - Security and resilience
Chips Act	CHIPS R&D Metrology Program (NIST), EN 17640, ISO/IEC 15408, CENELEC JTC 13 WG3.
5G, IoT	3GPP TR 33.894 V0.5.0 (2023-02), ETSI EN 303 645 Cybersecurity for Consumer IoT, ISO /IEC 20000, ISO/IEC 27033, IPv6, MANRS, IoT-RFC-9200, RFC-8613, ACE-OAuth framework, EDHOC, ECHC, GSMA/3GPP, GSMA SAS-UP/SAS-SM

CER Directive: Critical Entities Resilience Directive; NIS Directives: security of Network and Information Systems European Directives; CRA: Cyber Resilience Act; ENISA: European Union Agency for Cybersecurity; EUCC: European Cybersecurity Certification Scheme; EUCS: European Cloud Certification Scheme; ISO/IEC: International Organization for Standardization/International Electrotechnical Commission; ETSI: European Telecommunications Standards Institute; CEN: European Committee for Standardization;CI: Critical Infrastructure; IACS: International Association of Classification Societies; TR: Technical Report; TS: Technical Specification; ANSI: American National Standards Institute; ISA: International Society of Automation; NCSC: National Cyber Security Centre; NIST-SP: National Institute of Standards and Technology Special Publication; BSI: British Standards Institution; OWASP: Open Web Application Security Project; NISTIR: National Institute of Standards and Technology Internal/Interagency Reports; CVRF: Common Vulnerability Reporting Framework; IAS/IEC: International Society of Automation/International Electrotechnical Commission; IWA 31:2020: International Workshop Agreement 31:2020; CAPEC MITRE: Common Attack Pattern Enumeration and Classification of MITRE; FISMA: Federal Information Security Modernization Act; STRIDE: Spoofing, Tampering, Repudiation, Information, Denial, Elevation; ATT&CK MITRE: Adversarial Tactics Techniques and Common Knowledge MITRE, CVE (MITRE): Common Vulnerabilities and Exposures (MITRE); EN: European Standards; CVSS 3.1 (FIRST): Common Vulnerability Scoring System version 3.1 of FIRST; OSV: Open Source Vulnerabilities; 3GPP: Third Generation Partnership Project; GSMA Network Equipment Security Assurance scheme: Groupe Speciale Mobile Association scheme on Network Equipment Security Assurance; IT: Information Technology; eIDAS: electronic Identification Authentication and Trust Services; CEN: European Committee for Standardization; EU AI cybersecurity certification scheme proposal: EU Artificial Intelligence cybersecurity certification scheme proposal; AI: Artificial Intelligence; CENELEC JTC: European Committee for Electrotechnical Standardization Joint Technical Committee; IoT: Internet of Things; IPv6: Internet Protocol version 6; MANRS: Mutually Agreed Norms for Routing Security; RFC-8613: Object Security for Constrained RESTful Environments; ACE-OAuth framework: Authentication and Authorization for Constrained Environments Framework; EDHOC: Ephemeral Diffie-Hellman Over COSE; ECHC: Elliptic Curve-based Hill Cipher (ECHC); GSMA SASUP/SAS-SM: Groupe Speciale Mobile Association Security Accreditation Scheme for UICC Production/ Security Accreditation Scheme for Subscription Management.

stakeholders. The European Cybersecurity Skills Framework (ECSF) of ENISA[7] aims to profile twelve typical cybersecurity professional roles along with their identified titles, missions, tasks, skills, knowledge

and competencies and facilitate individuals, employers, and providers of learning programs within the EU to bridge the gap between the cybersecurity professional workplace and learning environments. The work does not include relations to cybersecurity standards.

The literature reviews limited research work on security standardization classification. The work in[54] provides a narrative review of the most frequently used cybersecurity standards and frameworks based on existing research work and their application to assist organizations in selecting the cybersecurity standard that best fits their cybersecurity requirements. The work mainly differentiates cybersecurity standards from frameworks and does not further categorize them into cybersecurity conceptual groups. Syafrizal *et al.* group international cybersecurity standards into general, local regulation, and industry-specific standards and map the relationship between the literature review and future research[54]. The proposed classification does not consider aspects of stakeholders. It could be enriched with current trends (e.g., IoT security, blockchain-based cybersecurity, *etc.*). Tsohou *et al.* review, analyze and classify information security standards in the clauses of the ISO/IEC 27001:2005 to facilitate security practitioners in understanding the plethora of security standards[55,56]. The current work is limited to specific ISO/IEC standards and does not address other standardization activities of information security.

The necessity for organizations to adhere to multiple standards at once can be both expensive and labor-intensive. Striving to fulfill diverse requirements often results in confusion and a perceived disorder, particularly when conflicting or overlapping standards. In this paper, we propose a taxonomy to help organizations understand which, how, and when to use cybersecurity standards depending on the use.

TAXONOMY BUILDING BLOCKS

Taxonomy is a scheme of classification[57] that partitions a body of knowledge and identifies relationships among the pieces[58] of things, concepts, and principles that underlie such classification[8].

The proposed standards-based taxonomy is structured in a step-wised approach based on the NIS 2 Directive[17], JRC Cybersecurity Taxonomy[8], and ECSF[7]:

- Cybersecurity standards are distinguished into four conceptual pillars of different preferences of stakeholders and their purpose of use.

- Varying standards attributes identified (e.g., year, publication, *etc.*).

- Semantic rules, hierarchies (classes) and relations (properties) specified among the above taxonomy elements to develop an ontology formal knowledge representation.

Structure and main pillars

The proposed taxonomy aims to guide stakeholders (e.g., organizations, practitioners, and individuals) on which standard(s) are relevant for them. Relevance is determined by a *conceptual four-pillar classification*, as presented in Table 2:

The categories of pillars are described below [Figure 1]:

- **Pillar-I. Industrial Sectors:** Fifteen (15) industrial sectors (categories) are defined, according to their value and impact on the EU economy in case of their service disruption. The categorization relies on the EU NIS 2 Directive[17] operators of essential/important services distinction and JRC sectorial classification[8].

Table 2. Conceptual questions and pillars to identify relevant standards

Question	Conceptual Pillar	Conceptual Pillar Description
Q1: Where are you?	I. Industrial sector	Sector-specific (e.g., transport, finance, and healthcare)
Q2: Who are you?	II. Stakeholder Profile	Security-related professional roles, skills and competencies (e.g., CISO and Auditor)
Q3: What's your interest?	III. Security domain	Cybersecurity discipline (e.g., Anomaly Detection and Certification)
Q4: What's used?	IV. Applications and Technologies	It refers to the applications and technologies utilized by the stakeholder (e.g., IoT and AI)

AI:Artificial Intelligence; IoT: Internet of Things; CISO: Chief Information Security Officer.

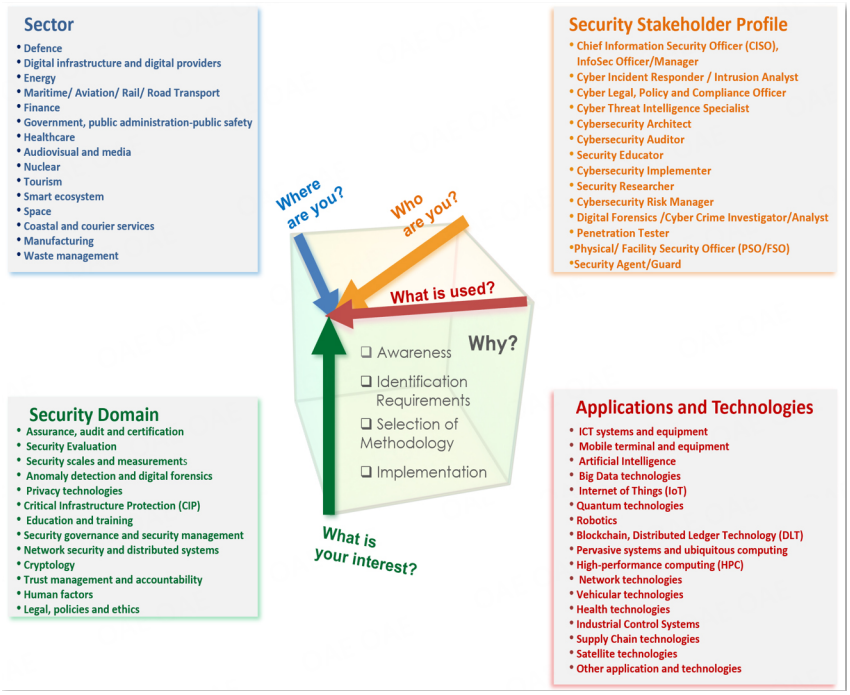

Figure 1. Overall view of the proposed standards-based taxonomy of security management.

- **Pillar-II. Stakeholder Profile:** It provides fourteen (14) different categories of expertise and/or professions related to cyber/physical security based on the ENISA ECSF report[7].

- **Pillar-III. Security Domain:** It refers to thirteen (13) security fields of knowledge (categories) from both cyber and physical aspects addressing existing security challenges of the EU economy[8].

- **Pillar-IV. Applications and Technologies:** It corresponds to seventeen (17) types of devices/data/techniques/technologies (categories) utilized by the stakeholder[8].

Since the stakeholder needs are identified in a quad selection set (options from the four pillars), the latter shall specify "why" the entity needs security standardization. Standard(s)/framework(s)/best practice(s) are distinguished into generic conceptual groups based on their content and purpose of use, as displayed in Table 3 and indicative examples presented in the following:

Table 3. Security management standards classification towards their purpose of use

Question	Purpose of Use	Content
Q5: Why do you need standardization?	Awareness	Cybersecurity terms, acronyms, and definitions supporting stakeholders' selections set
	Requirements identification	Elicit security requirements on a specific topic of interest
	Methodology	Select a suitable methodology on topics of security management
	Implementation	Specify and implement methodology/address requirements: guidance, directions, and best practices

- **ISO/IEC 27000 standard**[59] provides a basic vocabulary (Awareness) for information security management (Pillar-III), applied to ICT systems (Pillar-IV) by a Chief Information Security Officer (CISO, Pillar-II) in the Energy sector (Pillar I).

- **ISO/IEC 15408 standard**[28] provides the criteria (Requirements Identification) to *evaluate security properties* (Pillar-III) of *IoTs* (Pillar-IV), assessed by a *cybersecurity auditor* (Pillar-II) in *Healthcare* (Pillar-I).

- **The ETSI-Threat, Vulnerability, Risk Analysis (TVRA) technical specification**[22] or **ISO/IEC 18045 standard**[29] defines (Methodologies) the minimum actions performed by a *cybersecurity auditor* (Pillar-II) to conduct a *cybersecurity risk assessment* (Pillar-III) on *AI-based systems* (Pillar-IV) supporting *Maritime Transport* (Pillar-I) operations concerning the *evaluation criteria* (Pillar-III) prescribed in ISO/IEC 15408 standard.

- **ISO 28004 standard**[60] provides guidelines (Implementation) to an *ICS/SCADA Cybersecurity Analyst* (Pillar-II) in the *Manufacturing* sector (Pillar-I) for the *security management* (Pillar-IV) of supply chain systems (Pillar-IV), analyzing typical inputs/outputs of supply chain security requirements addressed in ISO 28000:2022[61] standard.

Considering the building blocks mentioned above, Figure 1 depicts the structure of the proposed taxonomy.

Semantic relations

The cybersecurity standards engage a set of attributes:

- **Range:** Indicates their applicability at the International, Regional (e.g., European) or National level.

- **ID/Version/Title/Year:** The standard/framework/best practice publication characteristics, i.e., its ID, version, title, and the year published.

- **Publisher/Technical Committee:** The Standardization Body, Policymaker, or other relevant party who developed/published the standard/frameworks/best practice (it can be an association of entities).

- **Purpose of Use (Why?):** Regarding the content, usage is specified following the classification described in Section Structure and Main Pillars Standard/frameworks/best practices can be mapped with one (1) or more purposes of use.

● **Type:** Concerning ISO and IEC technical processes[62] on standards lifecycle and their level of completeness, standards documents can be characterized by the following main types: a published standard, TR [TR is informative and non-normative, analyzing specific topics with complementary information (e.g., testing approaches, measurements, methodologies, and test cases).], Technical Specification (TS) [TS approaches an international standard in detail and completeness. Nevertheless, it has not yet passed through all approval stages (considering either premature or not reached consensus).], Approved Work Item (AWI), Publicly Available Specification (PAS) [PAS aims to boost standardization activity towards rapidly evolving technologies and respond to an urgent market need], treaty, best practice, or other type of guidance assigned by a relevant entity.

Upon stakeholder pre-defined selections in the taxonomy, a list of associated standards and their attributes are reported in a tabular structure, as depicted in Table 4.

All taxonomy elements, i.e., standards attributes, pillars, and purpose of use, are connected via semantic properties depicted in Table 5. Properties creating reciprocal relationships between two elements generate inverse relations (of inverse properties), e.g., "*Operates*" and "*isOperatedBy*", whereas some properties have a specific type of value, e.g., "*Integer*".

Concerning taxonomy hierarchies, the following semantic rules are identified:

• A *Pillar* (e.g., *"Pillar-III: Security Domain*") is a *classOf category* (e.g., "*Cryptology*"), whereas a *category* is *subclassOf Pillar*

• All *classes/subclasses* can have a set of *values/instances* (e.g., "*Cybersecurity_Standards*" *class* has "*ISOIEC15408*" *instance*)

• All *classes*, *subclasses* and *instances* can be *subjects* and *objects*, associated with *semantic properties*

• *Semantic properties* (e.g., "*Defines*", "*Supports*", *etc.*) are relationships between a *subject* (e.g., "*Cybersecurity_Standard*") and an *object* (e.g., "*Purpose_Of_Use*")

• Special characteristics of semantic relations between classes and/or instances (e.g., *Inverse* relations and *Integer* values) are expressed via *semantic properties*.

The proposed taxonomy is represented in semantic ontology structure using Web Ontology Language Version 2 (OWL 2) language of description logic and Resource Description Framework (RDF) in Protégé Open-source Ontology Editor[63]. It is built on the main taxonomy elements, described previously:

• the four conceptual pillars represent four superclasses embedding subclasses to address the corresponding categories, described in Section Structure and Main Pillars.

• attributes/types of standards and related reports are represented by five superclasses, i.e., range, type, (publication) characteristics, publisher/technical committee and purpose of use, containing subclasses to express the corresponding options, analyzed in Table 4.

Table 4. Template of standard attributes

Range	Type	Characteristics	Publisher/Technical committee	Purpose of use
(International/European/ Regional/ National)	(Standard/ TR/TS/PAS/ AWI/ framework/ best practice/ other)	(ID/Version/Title/Year)	(Standardization body/Policymaker, Other)	(Awareness/ Requirements identification/ Methodology/ Implementation)

TR: Technical Report; TS: Technical Spectification; PAS: Publicly Available Specification; AWI: Approved Work Item.

Table 5. Taxonomy's semantic relations

Semantic property	Semantic property further characteristics *(where applicable)*	Examples of semantic relations
Defines	-	a standard *Defines* another standard or best practice. Awareness report *Defines* all other reports (i.e., Requirements, Methodology, Implementation)
Implement	-	Applications and Technologies *Implement* Security Domain Best practices/guidelines *Implement* Requirements
Operates	Inverse (isOperatedBy)	Sector *Operates* Applications and Technologies Applications and Technologies are *OperatedBy* Security Stakeholder (inverse example)
Recommends	Inverse (isRecommendedBy)	Best practices *Recommend* methodologies and frameworks
ResidesIn	-	Security Stakeholder *ResidesIn* Sector
Evaluates	Inverse (isEvaluatedBy)	A Methodology *Evaluates* Requirements Security Domain *Evaluates* Applications and Technologies
Title	-	Cybersecurity Standards (e.g., ISO/IEC 15408) have *Title* Information, security, cybersecurity and privacy protection
Publisher	-	Cybersecurity Standards (e.g., 2700x related) have *Publisher* ISO and IEC
IdVersion	-	Information Security standard requirements have *IdVersion* ISO/IEC 27001
Year	Integer value	ISO/IEC 27001 Standard lastly published in *Year* 2022
Range	-	ISO 28001 *Range* is International

ISO/IEC: International Organization for Standardization/International Electrotechnical Commission.

• all classes may embed several individuals (instances of ontology's classes), e.g., "*Methodology*" class of "*Purpose of Use*" superclass contains the "*ISOIEC18045*" individual.

• all instances are connected via object properties with other instances or via data properties specific values (e.g., integer, Boolean, *etc.*) to declare their semantic relations [Table 5].

• all semantic rules previously described are followed in the current ontology.

Figure 2 illustrates the high-level structure of the OWL 2 ontology. Figure 3 depicts indicative ontology's individuals and semantic relations (properties) of Table 5 expressed in RDF framework. In Figure 3, the different colors in the arrows between individuals represent their connections with different properties, e.g., brown for property *Range* orange for property *Evaluates*. The pink arrows represent the relations between classes and individuals, e.g., class *"International" has Individual* "*ISOIEC15408*".

TAXONOMY APPLICATION

This section presents a use-case scenario considering specific criteria of stakeholders to illustrate the application of the proposed taxonomy. It describes the use-case scenario, and provides the generated results.

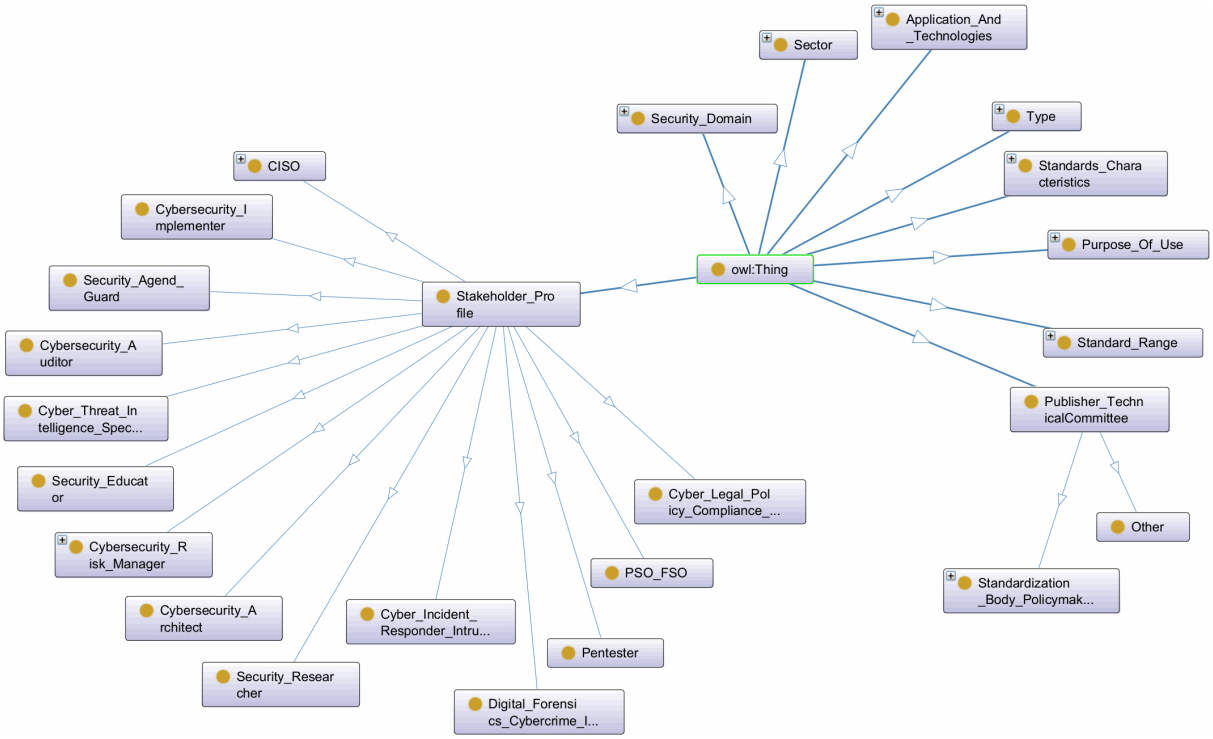

Figure 2. A snapshot of Cybersecurity Standards ontology high-level structure illustrating the Stakeholder's Profile and relations between classes. CISO: Chief Information Security Officer.

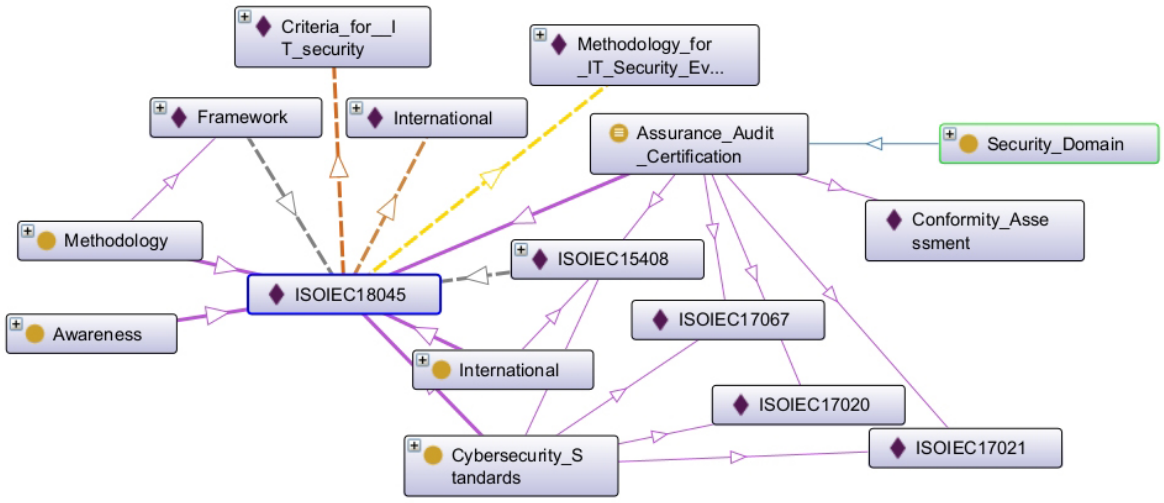

Figure 3. Cybersecurity Standards indicative instances depicting their semantic relations expressed via RDF semantic object and data properties in Protégé. ISO/IEC: International Organization for Standardization/International Electrotechnical Commission; CISO: Chief Information Security Officer; RDF: Resource Description Framework.

Scenario description

The interested party has answered the relevant conceptual questions Q1-Q4 (cf. Section "Structure and

Main Pillars) of the taxonomy as presented in the following, showing in italics the subsequent selections on the taxonomy, according to the scenario:

• Q1: He works in the Maritime Transport *(Pillar-I: Sector)*

• Q2: He is a/an CISO/InfoSec Manager *(Pillar-II: Security Stakeholder Profile)*

• Q3: Aiming to assess the organization's infrastructure for cyber risks and investigate whether the Target of Evaluation (TOE) meets cybersecurity requirements upon specified risk appetite and assurance level *(Pillar-III: Security Domain; the current scenario resides in the "Evaluation, Assurance, audit and certification" category)*

• Q4: The TOE is the vessel management system that utilizes AI Technologies and Machine Learning algorithms *(Pillar-IV: Applications and Technologies)*

Following the proposed taxonomy, the preferences on the conceptual pillars are depicted [Figure 4].

Concerning standards' purpose of use, all categories are relevant (e.g., requirements/methodology/implementation standards help assess risks, awareness standards in understanding the threat landscape).

Results

Novel AI-based technologies produce a wave of new diffused threats that cannot be holistically identified, prevented, and controlled as these technologies are still a new area of investigation. Future research could explore potential weaknesses and means to improve their security. Considering that emerging technologies can be partially protected, the AI technologies category (Pillar-IV) of the proposed taxonomy aims to gather information on prominent existing standards developed to address threats and vulnerabilities of AI systems and eliminate these security gaps. Standards/Frameworks/Best practices for AI-based systems are presented under two perspectives:

• standards and practices for utilizing AI technologies to secure interconnected systems (AI security)

• standards for securing AI-based systems (Secure AI).

The ETSI Industry Specification Group on Securing Artificial Intelligence (ISG SAI) has developed standards to preserve and improve the security of AI-based systems focusing on three topics:

• using AI to enhance security

• addressing attacks that leverage AI

• securing AI-based systems from attacks

AI-based Standards/Frameworks/Best Practices of the current results are generated considering the scenario pre-defined criteria (cf. Section "Scenario Description). The results of the overall taxonomy are depicted in a tabular structure, reflecting Standards/Frameworks/Best Practices and their attributes (cf. Section "Semantic Relations"), according to stakeholder's preferences (four pillars) and standards' purpose of use (cf. Section

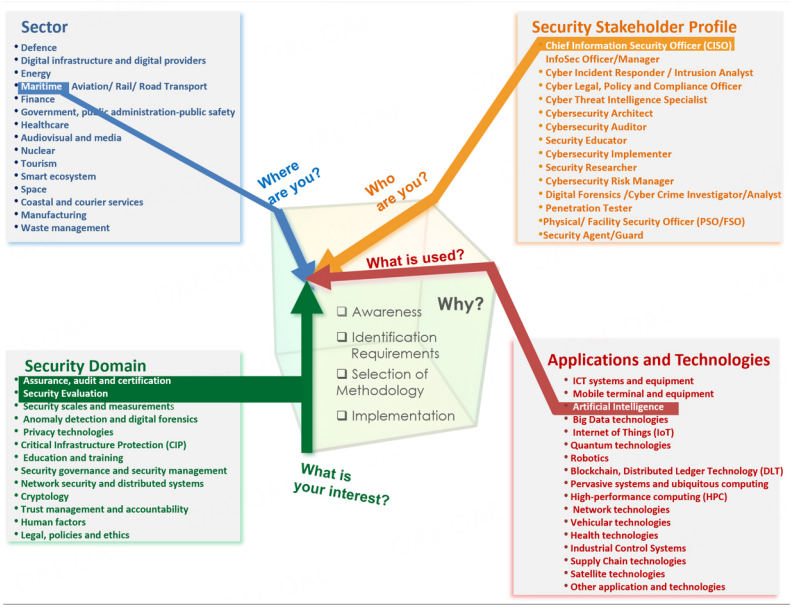

Figure 4. Quad selection of stakeholders on the conceptual pillars of the taxonomy to identify relevant Standards/Frameworks/Best practices for the security management of the TOE. TOE: Target Of Evaluation.

"Structure and Main Pillars"). Some of them were found in more than one pillar category. The results presented in Table 6 were prioritized following stakeholders' preferences (four pillars). Standards related to IT Evaluation and conformity assessment for Maritime Transport infrastructures, specifically for AI-based systems, are prioritized along with some indicative methodologies and frameworks proposed for adoption.

Figure 5 depicts instances of prominent standards/frameworks and best practices related to the topics of interest, derived from the respective ontology classes of "Maritime" (Pillar-I), "Security_Evaluation" (Pillar-III), and "AI" (Pillar-IV). The InfoSec Manager may consult them and decide which of them should adopt to cover the security needs of organizations.

CONCLUSIONS

Standards accelerate the security knowledge of stakeholders and practitioners, bring innovation, and increase their preparedness. Considering the digital transformation overload in modern societies and the rapidly improving malicious capacity of adversaries, the cybersecurity standardization effort has expanded globally. Nonetheless, the existing chaotic and exhaustive list of available security standards trying to capture multiple industry domains and technologies generates headaches for entrepreneurs. Research work on standardization classification and conceptualization is yet limited.

The current work explored the interplay between EU regulation and global or regional standards. Furthermore, it mapped well-known standards with the most important EU legal instruments in cybersecurity. Then, it developed a cybersecurity standards-based taxonomy aiming at facilitating businesses to easily comprehend the content, use and application of the various available cybersecurity standards. Moreover, stakeholders can utilize the taxonomy to get consulted on which cybersecurity standards they should adopt to protect their environments by answering a set of conceptual questions according to their specific goals and needs and receiving a list of standards that most fit with the security specificities and technical particularities of their environments. Our research work considers and enhances past cybersecurity standards classification and conceptualization approaches of prominent standardization

Table 6. Standards/Frameworks/Best practices delivered results towards stakeholder's pre-defined criteria

Range (International/Regional/European level)	Type (Standard/ TR/TS/PAS/ AWI/ framework/ best practice/ other)	ID/Version/Title/ Year	Publisher/Technical Committee (Standardization Body/ Policymaker, Other)	Purpose of Use	Pillar/Category
International	Standard	ISO/IEC 18045:2022 Methodology for IT Security Evaluation	ISO/IEC	Awareness/ Methodology	Maritime Transport Security Evaluation
International	Standard	ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection — Information security management systems — Requirements	ISO/IEC	Requirements Identification / Methodology	InfoSec Manager
International	TS	ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls	ISO/IEC	Methodology	InfoSec Manager
European	TS	ETSI TS 102 165-1 ETSI-TVRA (Threat Vulnerability Risk Analysis)	ETSI	Awareness/ Methodology	Security Evaluation
International	Standard	ISO/IEC 23894:2023 Information Technology-Artificial Intelligence-Guidance on risk management	ISO/IEC	Awareness/ Methodology	Secure AI
International	AWI	ISO/IEC AWI TS 5471: Artificial intelligence — Quality evaluation guidelines for AI systems	ISO/IEC	Implementation	Secure AI
International	AWI	ISO/IEC AWI TS 6254: Information technology — Artificial intelligence — Objectivesand approaches for explainability of ML models and AI systems	ISO/EC	Awareness/ Methodology	AI Security
International	Standard	IEEE P2807.1 - Standard for Technical Requirements and Evaluation of Knowledge	IEEE	Awareness/ Requirements Identification/ Methodology	AI Security
International	Guidance	AI RM Framework (2nd Draft September 2022)	NIST	Methodology	Secure AI, Security Evaluation
European	Standard	ETSI GR SAI 001 v1.1.1 (2022-01)	ETSI	Awareness/ Methodology	Secure AI
European	Standard	ETSI GR SAI 002 v1.1.1 (2021-08)	ETSI	Requirements Identification	Secure AI
European	Standard	ETSI GR SAI 005 v1.1.1 (2021-03)	ETSI	Methodology/ Implementation	Secure AI
International	Guidance	AI Policy Contributions (2022)	NIST	Implementation	Secure AI
International	Standard	ISO 28001/28002:2007 Security management systems for the supply chain - Best practices for implementing supply chain security, assessments, and plans - Requirements and guidance / Development of resilience in the supply chain	ISO	Awareness/ Requirements Identification / Implementation	InfoSec Manager

International	Standard	ISO 28003:2007 Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain security management systems	ISO	Awareness/ Requirements Identification	Assurance/Audit/ Certification
International	Standard	ISO 20858:2007 Port facility security assessments and security plan development	ISO	Awareness/ Methodology	Maritime Transport
International	Certification	Onboard ship certification	DNV	Requirements Identification	Maritime Transport
International	Standard	ISO/IEC 17067:2013 - Conformity Assessment - Fundamentals of product certification and guidelines for product certification schemes	ISO/IEC	Awareness/ Methodology	Security Evaluation Assurance/Audit/ Certification
International	Standard	ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems	ISO/IEC	Awareness/ Identification of Requirements	Assurance/Audit/ Certification
International	Standard	ISO/IEC 17020:2012 Conformity assessment - Requirements for the operation of various types of bodies performing inspection	ISO/IEC	Awareness/ Identification of Requirements	Assurance/Audit/ Certification
European	Best Practices	Cyber Risk Management for Ports (2020)	ENISA	Methodology/ Implementation	Maritime Transport
European	Best Practices	Port Cybersecurity - Good practices for cybersecurity in the maritime sector (2019)	ENISA	Awareness/ Methodology/ Implementation	Maritime Transport
International	TR	ISO/IEC TR 15443: 2012 Security Assurance Framework	ISO/IEC	Awareness/ Methodology	Assurance/Audit/ Certification
International	TR	ISO/IEC TR 15446:20- Information Technology-Security techniques	ISO/IEC	Implementation	Assurance/Audit/ Certification
International	Standard	ISO/IEC DIS 27006-1 Requirements for bodies providing audit and certification of information security management systems	ISO/IEC	Requirements Identification	InfoSec Manager
International	Standard	ISO/IEC 27014:2020 Information security, cybersecurity, and privacy protection — Governance of information security	ISO/IEC	Methodology	InfoSec Manager
International	Standard	ISO/IEC 27021:2017 Information technology - Security techniques - Competence requirements for information security management systems professionals	ISO/IEC	Requirements Identification	InfoSec Manager

TS: Technical Spectification; AWI: Approved Work Item; IEEE: Institute of Electrical and Electronics Engineers; AI: Artificial Intelligence; SAI: Securing Artificial Intelligence; TR: Technical Report; AI RM Framework: AI Risk Management Framework; InfoSec: Information Security; DIS: ISO/IEC Draft International Standard; DNV: Det Norske Veritas.

bodies, security communities and legal instruments[6-8,17] by developing a hierarchically structured conceptual model of cybersecurity standards based on a fourth-dimension classification that considers a set of stakeholders' characteristics, technologies, and their environment. In addition, we developed a semantic

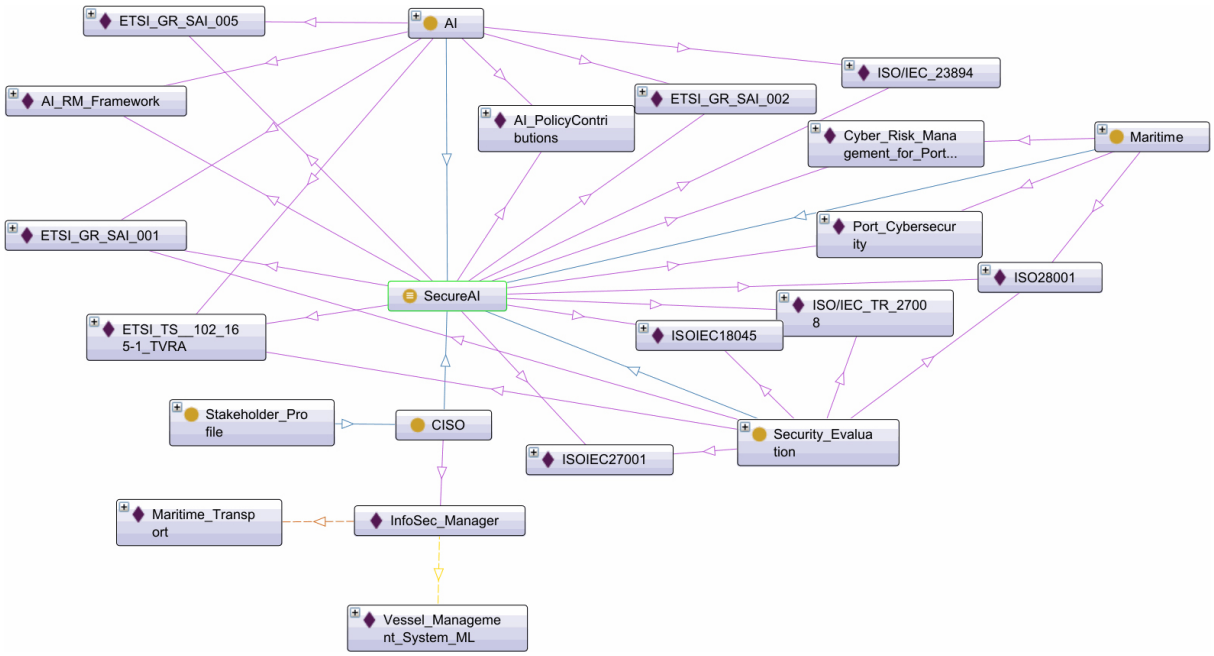

Figure 5. A combination of cybersecurity standards, frameworks and best practices related to security evaluation of AI/ML-based infrastructures together with sectorial cybersecurity guidelines for maritime transport. AI: Artificial Intelligence.

ontology to represent knowledge flows of different conceptual groups via semantic relationships following ontology engineering approaches (i.e., OWL 2 and RDF). Moreover, we presented a focused, realistic scenario to illustrate the applicability of taxonomy to security needs of stakeholders.

Future work could enhance the developed taxonomy with further semantic assertions and instances. Eventually, a semantic RDF-based query language could be used [i.e., Simple Protocol and RDF Query Language (SPARQL)] to validate the content of the taxonomy.

DECLARATIONS

Acknowledgments

The authors would like to thank all partners of the EU projects CUSTODES and SENTINEL. Special thanks to the University of Piraeus Research Centre for its continuous support. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Authors' contributions

Made substantial contributions to conception and design of the study and performed data analysis and interpretation: Kalogeraki EM

Performed data acquisition and provided administrative, technical, and material support: Polemi N

Availability of data and materials

Not applicable.

Financial support and sponsorship

This work has received funding from the European Union's Horizon Innovation Action program under grant agreement No. 101120684 project CUSTODES; In addition, it is supported by the European Union's

Horizon Research and Innovation program under grant agreement No101021659 project SENTINEL.

Conflicts of interest
All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Copyright

REFERENCES
1. Shafin SS, Karmakar G, Mareels I. Obfuscated memory malware detection in resource-constrained iot devices for smart city applications. *Sensors* 2023;23:5348. DOI PubMed PMC
2. Kara I, Aydos M. The rise of ransomware: forensic analysis for windows based ransomware attacks. *Expert Systems with Applications* 2022;190:116198. DOI
3. Maurer T, Nelson A; International Monetary Fund. The global cyber threat. Available from: https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm [Last accessed on 25 Apr 2024].
4. European Parliament and Council. Regulation (EU)2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing regulation (EU) No 526/2013 (cybersecurity act). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881 [Last accessed on 25 Apr 2024].
5. European Commission. Internal market, industry, entrepreneurship and SMEs. Available from: https://single-market-economy.ec.europa.eu/single-market/european-standards_en [Last accessed on 25 Apr 2024].
6. Eckmaier R, Fumy W, Mouille S, et al; European Union Agency for Cybersecurity. Risk management standards: analysis of standardisation requirements in support of cybersecurity policy. Available from: https://op.europa.eu/en/publication-detail/-/publication/df32fe7f-dc9d-11ec-a534-01aa75ed71a1/language-en [Last accessed on 25 Apr 2024].
7. ENISA. European cybersecurity skills framework (ECSF). Available from: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles/@@download/fullReport [Last accessed on 25 Apr 2024].
8. Nai Fovino I, Neisse R, Lazari A, Ruzzante G, Polemi N, Figwer M. European cybersecurity centres of expertise map-definitions and taxonomy. Available from: https://op.europa.eu/en/publication-detail/-/publication/07c5b4c0-b656-11e8-99ee-01aa75ed71a1 [Last accessed on 25 Apr 2024].
9. CEN and CENELEC European Standards. What is a standard? Available from: https://www.cencenelec.eu/european-standardization/european-standards [Last accessed on 25 Apr 2024].
10. European telecommunications standards institute (ETSI). Available from: https://www.etsi.org [Last accessed on 25 Apr 2024].
11. CEN and CENELEC European Standards. Types of deliverables. Available from: https://www.cencenelec.eu/european-standardization/european-standards/types-of-deliverables/ [Last accessed on 25 Apr 2024].
12. Kalogeraki E, Papastergiou S, Panayiotopoulos T. An attack simulation and evidence chains generation model for critical information infrastructures. *Electronics* 2022;11:404. DOI
13. Cisco. The internet of everything. IoE value index study. Available from: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-faq.pdf [Last accessed on 25 Apr 2024].
14. Di Franco F. Analysis of the European R&D priorities in cybersecurity Strategic priorities in cybersecurity for a safer Europe. Available from: https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity/ [Last accessed on 25 Apr 2024].
15. ENISA Research and Innovation Brief. Artificial intelligence and cybersecurity research. Available from: https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research [Last accessed on 25 Apr 2024].
16. Soler Garrido J, Fano Yela D, Panigutti C, et al. Analysis of the preliminary AI standardisation work plan in support of the AI Act. Available from: https://op.europa.eu/en/publication-detail/-/publication/b14d9c86-faa3-11ed-a05c-01aa75ed71a1/language-en [Last accessed on 25 Apr 2024].
17. EUR. Directive (EU) 2022/2555 of the European parliament and of the council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending regulation (EU) No 910/2014 and directive (EU) 2018/1972, and repealing directive (EU) 2016/1148 (NIS 2 Directive) (text with EEA relevance). Available from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj [Last accessed on 25 Apr 2024].
18. Official journal of the European Union. Directive (EU) 2022/2557 of the European parliament and of the council of 14 December 2022

on the resilience of critical entities and repealing council directive 2008/114/EC (text with EEA relevance). Available from:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557&qid=1691105450257 [Last accessed on 25 Apr 2024].

19. EUR. Proposal for a regulation of the EU parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 [Last accessed on 25 Apr 2024].
20. ETSI. Cyber security (CYBER); Implementation of the revised network and information security (NIS2) directive applying critical security controls. Available from: https://cdn.standards.iteh.ai/samples/63989/c249c46a4f66419fbc0234515f29e319/ETSI-TR-103-866-V1-1-1-2023-02-.pdf [Last accessed on 25 Apr 2024].
21. CEN CENELEC. Security standardization matters. Available from: https://www.cencenelec.eu/media/CEN-CENELEC/News/Publications/2020/2020-11-23_brochure_security.pdf [Last accessed on 25 Apr 2024].
22. ETSI. Cyber, methods and protocols. part 1: method and pro forma for threat, vulnerability, risk analysis (TVRA). Available from: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf [Last accessed on 25 Apr 2024].
23. Kyranoudi P, Kalogeraki EM, Michota A, Polemi N. Cybersecurity certification requirements for supply chain services. 2021 IEEE Symposium on Computers and Communications (ISCC); Athens, Greece, 2021, pp. 1-7.
24. ENISA. Cybersecurity certification EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS. Available from: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1 [Last accessed on 25 Apr 2024].
25. Commission implementing regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of regulation (EU) 2019/881 of the European parliament and of the council as regards on the adoption of the European common criteria-based cybersecurity certification scheme (EUCC). Available from: https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj [Last accessed on 25 Apr 2024].
26. ENISA. EUCS - cloud service scheme: EUCS, a candidate cybersecurity certification scheme for cloud services. Available from: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme [Last accessed on 25 Apr 2024].
27. ENISA. 5G cybersecurity certification scheme. Available from: https://www.enisa.europa.eu/topics/certification/copy_of_adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification/ad-hoc-working-group-on-5g-cybersecurity-certification [Last accessed on 25 Apr 2024].
28. ISO/IEC 15408-1:2022 international standard. Information security, cybersecurity and privacy protection - evaluation criteria for IT security. Available from: https://www.iso.org/standard/72891.html [Last accessed on 25 Apr 2024].
29. ISO/IEC 18045:2022 international standard. Information security, cybersecurity and privacy protection - evaluation criteria for IT security - methodology for IT security evaluation. Available from: https://www.iso.org/standard/72889.html [Last accessed on 25 Apr 2024].
30. ISO/IEC 17065:2012 international standard. Conformity assessment - requirements for bodies certifying products, processes and services. Available from: https://www.iso.org/standard/46568.html [Last accessed on 25 Apr 2024].
31. ETSI EN 303 645v 2.1.1.. CYBER; Cyber security for consumer internet of things: baseline requirements. Available from: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf [Last accessed on 25 Apr 2024].
32. Fagan M, Megas K, Watrobski P, Marron J, Cuthill B; NIST IR 8425. Profile of the IoT core baseline for consumer IoT products). Available from: https://csrc.nist.gov/pubs/ir/8425/final [Last accessed on 25 Apr 2024].
33. 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). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Last accessed on 25 Apr 2024].
34. 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. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG [Last accessed on 25 Apr 2024].
35. European Commission. Proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/EC (regulation on privacy and electronic communications). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 [Last accessed on 25 Apr 2024].
36. EN 17529:2022. Data protection and privacy by design and by default. Available from: https://standards.iteh.ai/catalog/standards/cen/7988285e-71fa-4a6b-845c-71ddadb1e33f/en-17529-2022 [Last accessed on 25 Apr 2024].
37. ISO/IEC 33001:2015 international standard. Information technology - process assessment - concepts and terminology. Available from: https://www.iso.org/standard/54175.html [Last accessed on 25 Apr 2024].
38. CEN ISO/IEC/TS 27006-2:2022. Requirements for bodies providing audit and certification of information security management systems - part 2: privacy information management systems (ISO/IEC TS 27006-2:2021). Available from: https://standards.iteh.ai/catalog/standards/cen/e97266b2-de16-49e1-9853-625f1a96ac04/cen-iso-iec-ts-27006-2-2022 [Last accessed on 25 Apr 2024].
39. ISO/IEC 27701:2019 international standard. Security techniques - extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - requirements and guidelines. Available from: https://www.iso.org/standard/71670.html [Last accessed on 25 Apr 2024].
40. European Commission. Data act: commission welcomes political agreement on rules for a fair and innovative data economy. Available

from: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491 [Last accessed on 25 Apr 2024].
41. Regulation (EU) 2022/868 of the European parliament and of the council of 30 May 2022 on European data governance and amending regulation (EU) 2018/1724 (data governance act). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868 [Last accessed on 25 Apr 2024].
42. European Commission. European chips act. Available from: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en [Last accessed on 25 Apr 2024].
43. CEN CENELEC. Stakeholders' workshop on trusted chips: standardization landscape and opportunities for Europe. Available from: https://www.cencenelec.eu/news-and-events/news/2022/brief-news/2022-12-05-stakeholders-workshop-on-trusted-chips/ [Last accessed on 25 Apr 2024].
44. Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts. Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF [Last accessed on 25 Apr 2024].
45. CEN/CLC/JTC 21. Artificial intelligence. Available from: https://standards.iteh.ai/catalog/tc/clc/f2e11393-2c03-4a0a-9bc4-92326e0118fc/cen-clc-jtc-21 [Last accessed on 25 Apr 2024].
46. ENISA. EU cybersecurity certification. Available from: https://certification.enisa.europa.eu/ [Last accessed on 25 Apr 2024].
47. European Commission. Proposed regulation on the cyber solidarity act. Available from: https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act [Last accessed on 25 Apr 2024].
48. ISO/IEC 27035-1:2023 international standard. Information technology - information security incident management - part 1: principles and process. Available from: https://www.iso.org/standard/78973.html [Last accessed on 25 Apr 2024].
49. Cichonski P, Millar T, Grance T, Scarfone K. Computer security incident handling guide recommendations of the national institute of standards and technology. Available from: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf [Last accessed on 25 Apr 2024].
50. Joint communication to the European parliament and the council. The EU's cybersecurity strategy for the digital decade. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018 [Last accessed on 25 Apr 2024].
51. Rutkowski A. Global standards collaboration: is it possible? Available from: https://circleid.com/posts/20230203-global-standards-collaboration-is-it-possible [Last accessed on 25 Apr 2024].
52. Abdelkafi N, Bekkers R, Bolla R, Rodriguez-Ascaso A, Wetterwald M. Understanding ICT standardization - principles and practices. Available from: https://pure.tue.nl/ws/portalfiles/portal/192511633/Slideset_Understanding_ICT_Standardization.pdf [Last accessed on 25 Apr 2024].
53. Taherdoost H. Understanding cybersecurity frameworks and information security standards-a review and comprehensive overview. 2022;11:2181. *Electronics* 2022;11:2181. DOI
54. Syafrizal M, Selamat SR, Zakaria NA. Analysis of cybersecurity standard and framework components. Available from: https://d1wqtxts1xzle7.cloudfront.net/78607584/426-libre.pdf?1642083233=&response-content-disposition=inline%3B+filename%3DAnalysis_of_Cybersecurity_Standard_and_F.pdf&Expires=1714029973&Signature=GfPbylQeBMrWwBVhMxV9PRYeVsPq6-vy25hETTDRHKMAdZ4x3xWpsUwxXjkOy8exhg8ofhgsmIbj7mKlSCXSoxDmJxb0viQHpNxjmQnZHkv8dqqzsg1BjMMw3JYmMVels9Eg~5iruj262U5m~jfZFFC73QuvGMozwDbPQlEcLjNE7A0QVcOrurB9qOWiV3PJ3eTV1jXXq439pyaNxQpnlchsXZCjcy5Zf3iHdlgXm34u3yi5mR7o5SdMa8wOpIJ2NsQpvwgXxR~GOeqbLd97y50bJOv8SP8bNHMDQ-ZQwjFxa2rbOKCF96qLORd6lnf2NgvxGsgfPdyX7jKAJ-Z0YQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA [Last accessed on 25 Apr 2024].
55. Tsohou A, Kokolakis S, Lambrinoudakis C, Gritzalis S. Information systems security management: a review and a classification of the ISO standards. In: Sideridis AB, Patrikakis CZ, editors. Next Generation Society. Technological and Legal Issues. Berlin: Springer Berlin Heidelberg; 2010. pp. 220-35.
56. Information technology laboratory, computer security resource center. NIST glossary. Available from: https://csrc.nist.gov/glossary/term/standard [Last accessed on 25 Apr 2024].
57. ISO/IEC/IEEE 21841:2019 international standard. Systems and software engineering - taxonomy of systems of systems. Available from: https://www.iso.org/standard/71957.html. [Last accessed on 25 Apr 2024].
58. ISO/IEC 27000:2018 international standard. Information technology - security techniques - information security management systems - overview and vocabulary. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en. [Last accessed on 25 Apr 2024].
59. ISO 28004-1:2007 international standard. Security management systems for the supply chain guidelines for the implementation of ISO 28000-Part 1: general principles. Available from: https://www.iso.org/standard/44962.html. [Last accessed on 25 Apr 2024].
60. ISO 28000:2022 international standard. Security and resilience - security management systems - requirements. Available from: https://www.iso.org/standard/79612.html [Last accessed on 25 Apr 2024].
61. International Electrotechnical Commission (IEC). Technical specification and publicly available specification. Available from: https://www.iec.ch/publications/specifications. [Last accessed on 25 Apr 2024].
62. A free, open-source ontology editor and framework for building intelligent systems. Available from: https://protege.stanford.edu/ [Last accessed on 25 Apr 2024].