Franco Martins, B.; Serrano-Gil, LJ.; Reyes Román, JF.; Panach, JI.; Pastor López, O.; Hadad, M.; Rochwerger, B. (2022). A framework for conceptual characterization of ontologies and its application in the cybersecurity domain. Software & Systems Modeling. 21(4):1437-1464. https://doi.org/10.1007/s10270-022-01013-0

Noname manuscript No.
(will be inserted by the editor)

A Framework for Conceptual Characterization of Ontologies and Its Application in the Cybersecurity Domain

Beatriz Franco Martins 0000-0001-9190-1047 ·

Lenin Javier Serrano Gil 0000-0002-1631-7139 ·

José Fabián Reyes Román 0000-0002-9598-1301 ·

José Ignacio Panach 0000-0002-7043-6227 ·

Oscar Pastor 0000-0002-1320-8471 ·

Moshe Hadad ·

Benny Rochwerger

Received: date / Accepted: date

Abstract Organizations are actively seeking efficient solutions for the management and protection of their assets. However, Cybersecurity is a vast and complex domain, especially for large enterprises because it requires an interdisciplinary approach. Knowledge Graphs are one of the mechanisms that organizations use to explore security among assets and possible attacks. The grounding of concepts is fundamental to implementing Knowledge Graphs, and it is one of the most relevant ontology applications. Therefore, Cybersecurity Ontologies have emerged as an important research subject. The first contribution of this paper is a search for previously existing works that have defined Cybersecurity Ontologies. We found twenty-eight ontologies in this search. Based on this result, we propose a Cybersecurity Terminological Validation and a Framework for Classifying Ontologies. Then, we provide a cross-analysis of these two proposals and present a proposal of best practices for improving the ontological approach in the cybersecurity domain. We also discuss the

In Memoriam and in honor of the first author's beloved father Engr. Hélio Brandão Martins M.D., who passed away during the research and publication of this work.

Valencian Research Institute for Artificial Intelligence (VRAIN), Universitat Politècnica de València, Camino de Vera s/n, 46022 Valencia, Spain, E-mail: {bmartins, lserrano, jreyes}@pros.upv.es,opastor@dsic.upv.es ·
Ingeniería de Sistemas e Informática, Universidad Pontificia Bolivariana, Km 7 via Bucaramanga Piedecuesta, Santander, Colombia ·
Escola Tècnica Superior d'Enginyeria, Universitat de València, Avinguda de l'Universitat, 46100 Burjassot, Valencia, E-mail: joigpana@uv.es ·
Accenture Israel Cyber R&D Lab, Tel Aviv, Israel, E-mail: {moshe.hadad, benny.rochwerger}@accenture.com

impact of this proposal with regard to the Ontology Engineering process. Our goal is to provide a solution that meets the organization's needs in terms of Cybersecurity and to contribute to Ontology Engineering research.

Keywords Conceptual Modeling · Ontology Classification · Cybersecurity Ontology · Ontology

1 Introduction

Organizations are actively seeking efficient solutions for the management and protection of their assets. However, Cybersecurity is a constantly evolving domain that is continually adopting new technologies and bringing major concerns to organizations. The security requirement community addresses this challenge by using graph approaches that provide practical mechanisms of analysis [90]. To deal with this challenge, there is a proposal known as Attack Graph (AG) [41], which is a kind of Knowledge Graph (KG) [44]. The Attack Graph aims to explore security among assets and possible attacks (i.e., risks). From another perspective, Conceptual Modeling, more specifically the branch of ontologies in computer and information sciences, has been a tool that is used to deal with elements constituting a conceptualization of a given domain [31]. Ontologies allow modelers to articulate abstractions of a particular state of affairs in reality. Indeed, cybersecurity KGs are implementations of conceptualizations that attempt to provide data analysis. In other words, a KG may be considered as an *Operational Ontology* [36]. In this sense, ontologies are a natural choice for providing the grounding for KGs.

The grounding of concepts is one of the most relevant ontology applications [31]. This comes from Guarino's perception about the *Ontological Level* [30], where the meaning of each concept is constrained in a formal way in order to provide a better conceptual approximation in describing a domain in reality. Moreover, the Ontological Level reflects a specific *Ontological Commitment* [31] regarding a particular axiomatization choice – in a language of representation. A language is made by symbols that express certain knowledge, and their combinations define the syntax of that language. Modeling languages, which usually use graphical representations, require the definition of rules and primitives that compose their *abstract syntax*. However, this is not enough to provide an intelligible conceptualization, and languages must clearly express the desired meaning of their constructs. Thus, the notion of *Ontological Commitment* is fundamental [36]. This means that, regardless of whether or not it is explicit, each concept in a modeling language commits to a specific notion in reality. Guarino formalized this idea in [31], and Guizzardi extended it in [36].

In addition to the representation issues about a real-world domain of knowledge as a model, it is still necessary to deal with the intrinsic difficulties of the domain itself. The misinterpretations and misunderstandings of the conceptualization are problems that enterprises must deal with; in fact, these are major when the involved domain is complex and constantly evolving. An example is the concept of *Risk* that we discuss throughout this document where different stakeholders may conceptualize the same term differently, even in the same enterprise scenario. This may include the stakeholders involved with the Ontology Engineering process, and their interests usually

interfere with the conceptualizations involved. There are two central groups working directly with the conceptualizations during the Ontology Engineering process: the domain specialists and the ontology engineers. In this case, specialists in the cybersecurity domain support the development of the ontology; therefore, they have the *Domain Perspective*, i.e., the *Cybersecurity Perspective*. Meanwhile, the ontology engineers must capture the domain notions provided by the domain specialists (cybersecurity specialists) providing them with conceptualization solution through ontological artifacts (documents, models, and implementations). The *Ontological Perspective* must comply with the *Domain Perspective* and the organizational requirements.

Since interoperability between systems is a mandatory requirement for organizations, this issue can have unpredictable side effects, especially when it comes to cybersecurity. Therefore, both the domain specialists and the ontology engineers responsible for conceptual modeling must have a clear understanding of the domain concepts. The conceptual modeling through an ontological approach is essential in making concepts explicit and in facilitating human comprehension about them [24]. Therefore, the main **goal** of this research is to combine the perspective of Cybersecurity Specialists with the perspective of Ontology Engineers, as follows:

1. the *Ontological Perspective* regarding the classification of the ontologies found, according to a framework that provides a homogeneous bases for comparison;
2. the *Cybersecurity Perspective* regarding the identification of the different terminologies used in existing ontologies (and their implementations as KGs) in order to determine their meanings.

The relationship between the terminology used in a certain domain of knowledge and its definitions (and consequent interpretation) is a common issue in all complex scenarios. These problems arise when it is necessary to ensure effective communication among humans, among systems, or between humans and systems [53]. For the cybersecurity domain, we proposed in [59] a search study for previous proposals that exist in the state of the art, their characterization, and analysis. This study provided results that we explore in Section 4 of this paper, and that motivated us to extend our proposal. Indeed, the initial state-of-the-art search that we made, composes the first step of the framework we propose. The framework defined in [59] presents a set of characteristics to compare Cybersecurity Ontologies. This work presents an extension of the initial characterization made in the pilot study. The extended characterization focuses on the interoperability among conceptualizations and the challenges to be faced concerning the two adopted perspectives. We present the detailed set of characteristics and the challenges involved in Section 5. Apart from the search of ontologies, we also present in Section 2 the state-of-the-art to find out similar approaches to ours. In other words, besides the study of the cybersecurity ontologies as part of the framework, we also study approaches for ontology classification regarding the framework as it is.

Throughout the process of comparing Cybersecurity Ontologies, we identify an additional issue. Although the best engineering approach could have been adopted to reach the understandability between domain specialists and ontology engineers, the resulting ontological artifacts have unclear, not covered concepts, or logical problems (Ontological Design Anti-patterns [38]). Moreover, the domain complexity is

potentialized by their own particularities besides the engineering process itself. Indeed, in line with this issue, the work [72] discusses the *Risk* concept (and *Risk-related* concepts) in the cybersecurity domain, comparing the notions of these concepts that practitioners use with the conceptualizations provided by the literature. The authors demonstrate that even among stakeholders who work within the same domain of knowledge, a clear conceptualization is still subject to divergences. The work also demonstrates that modelers (ontology engineers) usually rely on literature to get their notions about these studied concepts, further increasing the misunderstanding. This gap is an opportunity for additional research that still needs further studies, besides it encompasses a multidisciplinary research field concerning human relations and human-computer relations.

Under the Ontological Perspective, proposals for the classification of ontologies are vast [19, 25, 27, 36, 57, 42]. These proposals provide useful results when used simultaneously, despite having emerged in isolation from each other and with different objectives. The key result is to identify which is the ontological background used in conceptualizations (Ontological Perspective) besides the semantics used for defining their vocabulary (Domain perspective), putting together their stakeholder's viewpoints. A clear classification provides the required homogeneous scenario to achieve the FAIR principles (*Findability*, *Accessibility*, *Interoperability*, and *Reuse*) of digital assets [50]. Indeed, the pursuit to achieve the FAIR principles is essential for the Ontology Engineering process, as we discuss in Section 8. All in all, this motivated us to propose the **Framework for Classifying Ontologies** with the aim to provide a scenario where ontologies can be analyzed according to the same basis of comparison. Moreover, we intend to provide the stakeholders with a systematic and reproducible manner to do their ontological analysis.

The first contribution of this paper is the presentation of our **Framework for Classifying Ontologies**, which is from the *Ontological Perspective*. The objective focuses on analyzing the characteristics of the ontologies found in the state of the art (from our pilot study). We extend the approach through additional ontological classifications, refining our initial proposal [59]. The framework is based on several classifications for ontologies, providing a stratification for Cybersecurity Ontologies. The proposed framework's final classification is a criterion based on several well-known classifications for ontologies applied simultaneously and in an orthogonal way. A clear approach is essential to confer soundness because the interoperability process consists of elucidating the meanings of each term as a concept through an established common ontological landmark for all involved ontologies. We present the complete framework in Section 6.

We are also evolving the initial terminological verification of the pilot study into a Cybersecurity Terminological Validation covering the *Cybersecurity Perspective*. This work involves a set of terminological surveys that cover the main cybersecurity standards, in [87] we presented the first survey. The results of terminological validation provide a large amount of data; however, the presentation of these results is out of the scope of this paper. For this purpose, we developed a backend solution that we presented in [60, 61]. Our objective is to consolidate the meaning of the terms and support the ontological analysis process.

The second contribution uses the results to conduct a **Cross-analysis of the two perspectives** (Cybersecurity Perspective and Ontological Perspective). We combine both perspectives to increase semantic efficiency [1] in all possible implementations made on cybersecurity domain conceptualizations. In other words, this is a *Cross Ontological Analysis* approach that focuses on a standardization consensus together with its ontological grounding. The cross-analysis applied to multiple Cybersecurity Ontologies allows us to determine which cybersecurity concepts are most relevant to the ontology community, how they are (or should be) interpreted, and whether (or not) they are interoperable. Therefore, it is important to provide a proposal that promotes a holistic view that considers all involved stakeholders' perspectives without losing the global vision of promoting data interoperability. We present the cross-analysis in Section 7.

Finally, we conclude by discussing the impact of our approach on the Ontology Engineering process. We propose a set of best practices to the ontological approach in the cybersecurity domain, which is also applicable to other domains. For instance, despite the most recent progress in the Ontology Engineering process, there is no consensus about a methodological approach for the development of ontologies. Another challenge is to pursue the FAIR principles. These issues substantiate challenges such as the ones we detected through this study and faced throughout this paper.

We have organized the rest of this paper as follows: Section 2 presents other works that have compared ontologies. Section 3 describes the methodology we are using in our research. Section 4 presents some details and the results of our search for previous works in the field of cybersecurity ontologies. Section 5 proposes a classification of the previous works. Section 6 presents the evolved framework for classifying domain ontologies and their application on the studies we found. Section 7 presents a cross-analysis considering the two perspectives (cybersecurity and ontological). Section 8 discusses the results concerning the Ontology Engineering field and proposes some solutions to solve problems found in the previous works. Section 9 present our conclusions and discusses further research directions.

2 Related Works

This section describes other works related to the evaluation of domain ontologies in the cybersecurity context. There are already several studies that present proposals for ontologies in the cybersecurity domain, but only a few studies classify, analyze, or evaluate these proposals. The reason is that studies on this topic are recent, as well as their applications in cybersecurity. Therefore, we conducted a Targeted Literature Review (TLR). This approach only keeps the significant references to maximize rigorousness while minimizing selection bias. We apply our search string [2] in the most common digital libraries, Scopus, IEEEXplore, and ACM. The inclusion criteria were: (IC1) papers that classify cybersecurity ontologies (or parts of ontologies); and (IC2) papers that present frameworks or methods to classify cybersecurity-related ontologies (or parts of ontologies). The exclusion criteria were: (EC1) papers that do

[1] Semantic efficiency regarding the notions proposed in [38]

[2] Search string accessed on June 2020: (*ALL* = *"ontologies classification" OR "ontology classification"*)

not classify ontologies; (EC2) papers out of the scope of the cybersecurity domain; and (EC3) papers that could not be read. We made this search in August 2020.

The works we found in our search for related works were the first ones published focusing on Ontology-Driven Conceptual Modeling. We did not find any systematic literature review covering this specific domain. Below, we describe the papers that satisfied our parameters.

The survey in [91] presents a set of Security Ontologies that is classified into eight families. This classification is helpful in providing a general perspective. However, it is hard to use a homogeneous ontological analysis due to the mixed criteria adopted. For some ontologies, the focus is on the level of formalization (Security taxonomies), while others focus on the level of generality (General security ontologies or Specific security ontologies); some even use their domain aspects (Web-oriented security ontologies, Risk-based security ontologies, Ontologies for Security requirements, or Security modeling ontologies). Indeed, those authors demonstrated the link between fields of security requirement engineering and ontologies that require more study. Therefore, in Section 5, we show that this kind of classification requires an orthogonal approach, especially if the objective is to provide interoperability.

The study in [66] provides metrics concerning the evaluation of Cybersecurity Ontologies. However, similar to the work in [91] the evaluation criteria adopted is not clear despite being a very well-founded study. The study shows the complexity of the Cybersecurity domain and how complicated it is to define reliable and consensual semantics in this domain.

The work of Sikos [88] presents a literature review in the context of Cybersecurity Ontologies. This related work introduces multiple classifications, but the orthogonality relationship among them is not evident because, on many occasions, they tend to mix their classifications. Besides, the authors focus only on triple-stores using Resource Description Framework (RDF) [3] triples, setting aside Not Only SQL (NoSQL) platforms.

The work in [81] goes in the same direction as [88], but it focuses on the Ontology Web Language (OWL) [4] approach and presents a set of metrics under the formalization level perspective. In contrast, we make no distinction about the language or implementation used because we want to know any approach that brings the state of the art closer to the state of practice and not just those that focus on a single practical aspect (language or implementation).

Aside from the Cybersecurity domain, several works compare other domain ontologies; however, most focus the comparison criteria on conceptual matching. Their objective is to verify if a concept that is present in different ontologies has the same meaning by verifying formal characteristics (in the ABox [5]). The work of Keil [54] presents a summary of those approaches. Similarly, there are even proposals for tools to automate this task [107]. The systematic literature review in [10] covers the ontologies in the Security domain. Their comparison criteria also focus on implementation

[3] http://www.w3.org/TR/rdf-mt/

[4] https://www.w3.org/TR/owl2-syntax/

[5] ABox statements represent instances of associated concepts at the knowledge base.

in OWL, RDF, and DARPA Agent Markup Language (DAML) [6]. These approaches are different from ours since our focus is on conceptualization itself (in the TBox [7]). The work in [62] compares foundational ontologies. Although it is interesting from the ontological perspective that we consider, it deals with a higher level of abstraction. Thus, it is a job to consider within the Ontology Engineering process, which is out of the scope of our current research.

As a conclusion of the related works, we highlight that the few publications that focus on comparing Cybersecurity Ontologies do not classify the results into characteristics, and they use a reduced sample for the analysis. There is also a lack of best practices to classify cybersecurity ontologies. The following sections describe our proposals to cover all of these existing gaps.

3 Applied Methodology

In our research, we apply the Design Science Methodology [108] which is defined as "the design and investigation of *artifacts* in *context*". Our **final target** is to provide a solution (*the artifact*) able to facilitate the creation, management, and integration of KGs supported by a well-designed ontology. We are dealing with the domain of Cybersecurity (*the context*) focusing on the perspectives of Ontology and Software Engineering to produce an efficient solution. Figure 1 shows the research Engineering Cycle we use in our research according to the Design Science Methodology [108].

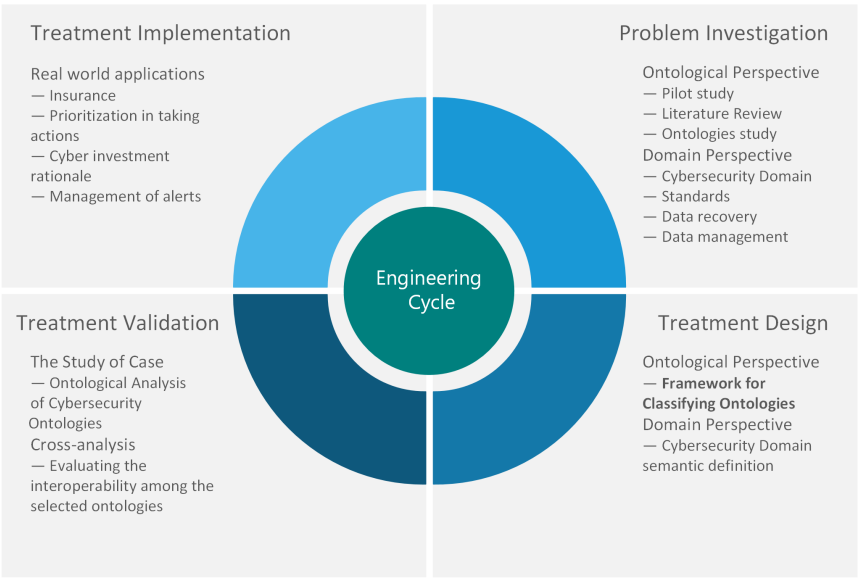


Fig. 1 Engineering cycle of our research.

[6] http://www.daml.org/

[7] TBox statements describe the domain by defining its concepts and relations.

The three first steps of the Engineering Cycle compose the Design Cycle and the last step that validates the solution using it in real-world scenarios. The Design Cycle presented in Figure 1 has the above steps:

Problem Investigation: The first step to achieving our final target is to know state-of-the-art ontologies covering the Cybersecurity domain if they provide KG implementations, and what are their technical approaches.

Treatment Design: Then, we focus on the treatment of the data we have obtained in the first step, including the definition of a clear method to compare domain ontologies (Cybersecurity Ontologies). This includes **the Framework for Classifying Ontologies** we propose (presented thought this paper) and managing the semantics information (vocabulary, terminology, data sources) of the domain.

Treatment Validation: We validate our proposal by classifying Cybersecurity Ontologies and consolidating their semantics through a cross-analysis process. In this paper, we illustrate the approach presenting the cross-analysis of the *Risk* concept, which is present in our study.

Completing the Engineering Cycle, the methodology has the below last step (also depicted in Figure 1):

Treatment Implementation: We intend to use our approach by applying it in real-world scenarios, with the support of Accenture LTD, a well-known software consulting that provides financial support for this project.

4 Conceptual Characterization of Cybersecurity Ontologies

We are dealing with a complex domain in both fields (Ontology and Software Engineering), to produce efficient KG management and interoperable solution. This complexity requires not only an investigation into similar approaches (as presented in Section 2) but also into the elements contained in these approaches; in this case, the domain ontologies themselves (Cybersecurity Ontologies). The research questions made to find out these ontologies are:

1. What are the existing works around Cybersecurity Ontologies?
2. What should include a well-grounded Cybersecurity Ontology?
3. What are the existing implementations, and what are their technical approaches?
4. Is there any additional relevant ontology that applies to our study?

This section describes the process of answering these questions by searching for existing ontologies of the cybersecurity domain in the state of the art, as part of the Problem Investigation of the Design Science methodology. We also summarize the results we found, grouping some found ontologies according to their conceptual characterization. Our objective in this research step is to identify proposals in the cross-field of Cybersecurity and Ontologies, evaluate the existing Cybersecurity Ontologies' applicability, and identify the possible data sources of cybersecurity information. For that, we cover both perspectives (Ontological and Domain).

4.1 Looking for Cybersecurity Ontologies in the Literature

We conduct a pilot study for the **Conceptual Characterization of Cybersecurity Ontologies** [59] searching for Cybersecurity Ontologies and providing them an initial classification. As well as presented in Section 2, the use of ontologies in Cybersecurity is recent, and there are few ontologies covering the broad of this domain; therefore, we conduct an initial TLR to search for those ontologies. We apply a succinct, but significant, search string [8], in the digital libraries ACM, Springer, IEEE, Scopus, and Google Scholar. We applied the selection criteria in three steps. In the first step, we focus on the publication title; in the second step, we read the abstract; and, in the third step, we read the whole document. The inclusion criteria were: (IC1) papers that present cybersecurity ontologies; and (IC2) papers that present parts of cybersecurity ontologies. The exclusion criteria were: (EC1) papers inaccessible for reading; (EC2) papers with low relevance by the number of citations; (EC3) papers that do not present effectively any proposal of ontology. At least two researchers carried out this work, one for each perspective: a domain specialist regarding Cybersecurity and an ontology engineer for the Ontological bias. The ontology engineer conducts all the search stages, and the domain specialist gives expert advice, typically on cybersecurity details and doubts clarification matters. We made this search in April 2020.

Although the used search string was limited, it was enough to look for the particularities of ontologies, like those presented in [88]. Indeed, we found that the knowledge base for cybersecurity can vary. On the one hand, we found more specific conceptualizations in which the domain focuses on parts such as “Malware”, “Vulnerabilities”, “Risks”, among others. On the other hand, we have also verified the existence of more generalist approaches, for example, dealing with risks in addition to the computational environment or dealing with security in general. Therefore, we observe the need to deepen the search for ontologies that cover all or parts (more general or more specific) of the cybersecurity domain. We start a Systematic Literature Review (SLR), which is still in progress, to eliminate the deficiencies detected in the search and facilitate greater traceability of the study; whose results will be reported in our future publications.

Taking to account the results of the pilot study (presented in [59]) and the classification criteria used, we upgrade this first round of search with the second round of search before starting the SLR. The second round of search is a TLR conducted in January 2021, using the same pilot study (first round) search string, and applying it again in the same digital libraries. We also use the same inclusion criteria (IC1 and IC2), but besides the original exclusion criteria (EC1, EC2, and EC3), we have added a fourth exclusion criterion (EC4) which removes from the selection all papers already selected in the first round.

However, we already knew in advance that this search result still would not be able to find two relevant works of our interest: the Common Ontology of Value and Risk (COoVR) [84], which is a well-grounded and more general ontology, and the

[8] Search chain: $(TITLE = \text{“Cybersecurity Ontology”})$ *or* $(\text{“Cybersecurity Ontologies”})$ when it is not possible to filter by title.

Ontology of ISO/IEC 27005:2011 [1] which is more specific focusing on another standard recognized by the cybersecurity community. Therefore, we manually add these two works to our selection.

Note that both, the pilot study (including its update as the second round of search and manual adds) and the SLR (in progress), are state-of-the-art research steps also part of the framework that we present in Section 6. Moreover, we use the framework to support the grouping choices we present throughout this section as the compilation of these two initial rounds of search results. From the first round (pilot study) of our state-of-the-art research, we detail here only two ontologies: the well-grounded ontology found and an operational ontology of our interest to provide a broader overview of our approach. However, all the ontologies found in the first round have their classification summarized, and their details are in the pilot study [59]. Regarding the papers found in the second round, we briefly describe each ontology (or sub-ontology) in Sub-sections 4.3, 4.2, 4.4, and 4.5. According to the established ontological perspective, we group all these ontologies by their most relevant characteristics. Additionally, we summarize the search results in Sub-section 4.6, providing a comparative frame of the found ontologies.

4.2 Reference Ontologies

One of the Reference Ontologies we found in the first round was the Conceptual Model of Vulnerability Ontology (CVO) [94]. This is an ontology-based conceptual model (a Reference Ontology) for the cybersecurity vulnerability domain (a Domain Ontology), which is a specific part of the cybersecurity universe. Thus, this ontology complies with information security standards and incorporates social media concepts. Subsection 4.4 provides new information about a recent extension of this ontology.

4.3 Operational Ontologies

MulVAL [78] (Multihost, Multistage, Vulnerability Analysis) is a framework that uses the Datalog language (a subset of Prolog) as the modeling language. As Prolog, Datalog consists of facts and rules, which are defined using predicates. This framework models the interaction of software bugs with the system and network configurations and provides a reasoning engine. The MulVAL framework can be considered to be an Application Ontology since it inbounds both a specific domain (Domain Ontology) and a set of tasks that scans new information from its network (Task Ontology). It uses the Open Vulnerability Assessment Language (OVAL) [9], which is an XML-based language for specifying machine configuration tests. The OVAL tool (an OVAL-compliant scanner) and the analyzer provide a vulnerability report and an output for the Datalog clauses.

In the second round of our search, we found other operational ontologies. Most of them focus on practical approaches. We detail these ontologies throughout this subsection.

[9] http://oval.mitre.org/documents/docs-03/intro/intro.html

The Cold-start cybersecurity ontology [23] provides an Operational Ontology for the cybersecurity vulnerability management domain from a framework that converts textual descriptions of software vulnerabilities into a formalized Domain Ontology. It is implemented in OWL and uses SWRL to define inference rules for implicit relations. However, there are no foundational grounding notions in terms of semantics.

The SecOrP Ontology [45] is an Operational Ontology. The authors formalize the ontology's main concepts following a bottom-up approach[10] to represent heterogeneous security tools from different vendors. The approach is a pragmatic proposal whose goal is to provide interpretability and interoperability of security tools through semantic annotations and reasoning. Again, the ontology is not grounded on any Foundational Ontology.

The Combined System Resilience-Cybersecurity Ontology [5] is a proposal of an Operational Ontology to identify and classify system threats, vulnerabilities, and risks. It provides reasoning from a combined schema that includes specific ontologies (or sub-ontologies) from engineering, security-specific vulnerability/threat/risk, and human behavior/social influence domains. However, the publication lacks information about formalization or ontological grounding.

The SEPSES Cybersecurity KG [55] is a Linked Data proposal that is implemented thought Triple Pattern Fragments (TPF), SPARQL , and RDF. This approaches uses Apache Jena to produce an Operational Ontology based on concepts from different cybersecurity glossaries (CWE [11], CVE [12], CAPEC [13], and CVSS [14]). Even thought, the resulting KG [15] provides a pragmatic approach, it also lacks ontological grounding.

The Cybersecurity Ontology for the CSKB [58] approach is an Operational Ontology that is implemented as a KG. The authors propose a practical approach to cluster heterogeneous' data using the Neo4J database. However, the reliability of the data depends on future additional classifications and recommendations of the data through inference algorithms. As with other practical approaches, this approach lacks ontological grounding.

The VulKG ontology [82] is an Operational Ontology written in OWL that is inspired by the UCO [95] and the IDS ontology [101]. We analyzed the UCO and the IDS ontology in the first round of the study [59]. Just as the ontologies that inspired it, the VulKG ontology has no strong foundational grounding and is based on the Linked Data [9] perspective.

The Ontology of ISO/IEC 27005 [1] is an Operational Ontology that aims to clarify the concepts provided by the ISO/IEC 27005:2011 [46] standard; it is an operational model in OWL that is implemented through the Protègè tool [16]. The ISO/IEC 27005:2011 standard does have a newer version, the ISO/IEC 27005:2018 [49]. However, the ontology does have no foundational ontology support.

[10] https://github.com/Chadni-Islam/Security-Ontology/blob/master/Ontology.jpeg
[11] https://cwe.mitre.org/
[12] https://cve.mitre.org/
[13] https://capec.mitre.org/
[14] https://www.first.org/cvss/specification-document
[15] https://sepses.ifs.tuwien.ac.at/
[16] https://protege.stanford.edu/

4.4 Operational Ontologies with a previous Reference Ontology

The Cyber Intelligence Alert System (CIA) [93] proposal is derived from an extension of the Conceptual Model of Vulnerability Ontology (CVO) [94] that we found in the first round of selection and the Cyber Intelligence Ontology (CIO) [93] found in the second round. While the CVO provides a representation of the cybersecurity vulnerability domain (a Domain Ontology), the CIO provides a conceptualization that deals with cybersecurity alerts (a Task Ontology). Together, the CVO and the CIO support the CIA System, which is an implemented solution (an Application Operational Ontology). This recent work changes the classification we made during the first round of study, providing more details. However, the proposal still lacks foundational grounding.

4.5 Well-grounded Ontology

In the first round of search, we found CRATELO [74, 76], which is a three-layer ontology [71] proposal for the domain of cybersecurity (Domain Ontology). The Foundational Ontology called DOLCE-spray [73], which is a simplification of the DOLCE ontology, grounds it. The CRATELO ontology also includes the Security Core Ontology (SECCO) and the Domain Ontology of cyber operations (OSCO). It is a well-grounded ontology that is implemented with OWL and SWRL [17] with Protègè. CRATELO has some extensions described in [75, 6].

In second round of search, we found the Common Ontology of Value and Risk [84] (COoVR), which is a *Reference Ontology* written in OntoUML [7] (an ODML) and grounded on UFO [34, 40]. Although this proposal has not been implemented, an operational version using gUFO (an implementation of UFO in OWL-DL) [3] is possible and viable. The ISO/IEC 27000:2018 [48] standard, which provides an overview of Information security management systems, supports this conceptualization. Since this standard has a general approach (about the security domain), the COoVR can be a basis for cybersecurity domain sub-ontologies through specializations.

4.6 Comparative Frame

We present in this subsection the summary of the ontology characterization that we made based on the criteria we proposed in [59]. In the first round of search conducted in April 2020, we found twenty-five papers (19 ontologies): 5 are only Reference Ontologies, and 20 are Operational Ontologies (4 of which are implementations supported by a Reference Ontology). Since some works refer to the same ontology, we found a total of nineteen ontologies. While in the second round of search conducted in January 2021, we found nine additional works (among them, 7 additional ontologies and 1 sub-ontology): only 1 work presents a Reference Ontology (well-grounded), 8 present Operational Ontologies (1 of which is an implementation supported by a

[17] https://www.w3.org/Submission/SWRL/

Reference Ontology). Two of the works added in the second round of search were added manually as they present proposals of our interest.

Table 1 shows the Level of Application classification results for the ontologies found.

Table 1 Level of Application of the studied ontologies.

Level of Application	**Number of Ontologies**			
	April 2020	**January 2021**	**Manual add**	**Total**
Reference Ontology	5	1 (0 additional)	1	6
Operational Ontology	20	8 (7 additional)	1	28
Operational Ontology supported by a Reference Ontology	*4*	*1*	*0*	*5*

Table 2 shows the Level of Generality classification results for the ontologies found.

Table 2 Level of Generality of the studied ontologies.

Level of Generality	**Number of Ontologies**			
	April 2020	**January 2021**	**Manual add**	**Total**
Domain Ontology	11	6	2	19
Task Ontology	0	0	0	0
Application Ontology	5	1 (sub-ontology)	0	5
Core Ontology	2	0	0	2
Ontology grounded over a Foundational Ontology	*4*	*1*	*0*	*5*

Considering the ontologies studied, we total the characterization made according to the proposed framework classification levels as depicts Table 3.

Table 3 Cybersecurity Ontologies' works selection process.

Search	**Number of Publications**			
	April 2020	**January 2021**	**Manual add**	**Total**
Papers found	198	229 (31 additional)	2	231
Papers inspected	32	48 (17 additional)	2	51
Papers excluded (EC1)	3	0	0	3
Papers excluded (EC2)	0	0	0	0
Papers excluded (EC3)	4	9	0	12
Papers excluded (EC4)	–	32	0	32
Papers included	25	8	2	35
Ontologies found	*19*	*8 (1 sub-ontology)*	*2*	*28*

The total number of ontologies that we found does not correspond to the number of publications because some publications refer to the same ontology and others refer to more than one ontology (or sub-ontology). At this stage of our research work, we found a total of twenty-eight ontologies that are refereed in thirty-five publications. Table 4 presents all the works extracted.

Table 4 Summary of Cybersecurity Ontology Characterization.

		Level of Application		Level of Generality	
Search	**Proposed Ontology**	**Reference Ontology**	**Operational Ontology**	**Well-grounded**	**According to [30, 104]**
Apr/20	CCS [69]	No	Yes	No	Domain
Apr/20	CoCoa [77]	Yes	Yes	No	Application
Jan/21	Cold-start Cybersecurity Ontology [23]	No	Yes	No	Domain
Jan/21	CSR-Cybersecurity Ontology [5]	No	Yes	No	Domain
Manual	COoVR [84]	Yes	No	Yes	Domain
Apr/20	CVO[18]- CIA System [94]	Yes	No	No	Domain
Jan/21	CVO & CIO - CIA System [93]	Yes	Yes	No	Application
Apr/20	CRATELO [74]	No	Yes	Yes	Application
Apr/20	CRATELO [76]	No	Yes	Yes	Domain
Apr/20	CRATELO [75]	No	Yes	Yes	Domain
Apr/20	CRATELO [6]	No	Yes	Yes	Domain
Apr/20	Cyber Ontology [79]	No	Yes	No	Application
Apr/20	Cybersecurity Ontology for Critical Infrastructures [8]	No	Yes	No	Domain
Jan/21	Cybersecurity Ontology for the CSKB [58]	No	Yes	No	Domain
Apr/20	IDS [101]	No	Yes	No	Core
Apr/20	IM [68]	No	Yes	No	Domain
Apr/20	IoTSec [67]	No	Yes	No	Domain
Apr/20	Cybersecurity Knowledge Base [51]	No	Yes	No	Domain
Apr/20	Malware Ontology [28]	Yes	No	No	Domain
Apr/20	MITRE Co approach [71]	No	Yes	No	Core
Apr/20	MulVAL [78]	No	Yes	No	Application
Jan/21	Ontology for the SEPSES KG Cybersecurity [55]	No	Yes	No	Domain
Apr/20	Ontology of Cybersecurity Operational Information [96]	Yes	Yes	No	Domain
Apr/20	Ontology of Cybersecurity Operational Information [98]	Yes	No	No	Domain
Apr/20	Ontology of Cybersecurity Operational Information [99]	Yes	Yes	No	Domain
Apr/20	Ontology of Cybersecurity Operational Information [97]	Yes	No	No	Domain
Manual	Ontology of ISO/IEC 27005 [1]	No	Yes	No	Domain
Apr/20	OVM [106]	Yes	Yes	No	Domain
Apr/20	POC [109]	No	Yes	No	Application
Apr/20	SCIC [17]	No	Yes	No	Domain
Jan/21	RMO Ontology [85]	No	Yes	No	Domain
Jan/21	SecOrP [45]	No	Yes	No	Domain
Apr/20	UCO [95]	No	Yes	No	Domain
Apr/20	VDO [11]	Yes	No	No	Domain
Jan/21	VulKG [82]	No	Yes	No	Domain

5 Characteristics for Comparing Cybersecurity Ontologies

Taking as input papers of the state of the art found in the previous section, we define two viewpoints: the *Ontological Perspective* as a conceptual modeling approach, and the *Cybersecurity Perspective* as a domain of knowledge specialists' viewpoint. The former looks at the semantic foundation, while the latter deals with the knowledge domain itself. When facing the problem from two different perspectives, we came across a series of issues. Below, we detail the characterization that we propose and the challenges to be faced.

Table 5 summarizes the characteristics we look for to extract and analyze ontologies in the works taking into account these adopted perspectives.

Table 5 Characteristics we look for to extract and analyze ontologies.

	Characteristics of the Cybersecurity Perspective
Terminological Verification	Using ISO/IEC 27032:2012 [47] and ISO/IEC 27000:2018 [48] standards.
Terminological Validation	Analysis of the definitions of the terms using additional cybersecurity standards.
	Characteristics of the Ontological Perspective
Framework to Classify Ontologies	Taking the an orthogonal approach for the proposals [31, 36, 104, 103, 26, 25, 102].

For the *Cybersecurity Perspective*, our study demonstrates that the initial **Terminological Verification** that we proposed in [59] was useful; however, there is no guarantee that the approach used in these cybersecurity ontologies achieves the security goals or allows interoperability [35]. We used the terminology that was defined in the ISO/IEC 27032:2012 [47] [19] and the ISO/IEC 270002018 [48] [20] standards (the vocabulary of these standards) applied to the papers we found in our state-of-the-art study. We evaluated the most frequently used terms (concepts) in the publications to compare which notions of cybersecurity each of the selected ontologies uses (e.g., if they all had the concepts like vulnerability, threat, risk, among others). We focused on these standards because they are appropriate for guiding the treatment of cybersecurity concepts [100].

The definitions used in standards such as those in ISO/IEC exist to clarify the interpretation of terms that are present in the domain of knowledge that they cover. However, the standards use natural (or technical) language that leaves room for more diverse interpretations. Besides, in the same domain of knowledge (or in overlapping domains), well-known standards may provide conflicting definitions for the same term, depending on the point of view taken. Thus, we also need to know the meanings, the context of use, and the importance of these terms. Therefore, we extended

[18] The same ontology called Conceptual Model of Vulnerability Ontology (CVO) in [59].

[19] ISO/IEC 27032 promotes procedures to establish and maintain security in cyberspace in the dimensions of *Confidentiality*, *Availability*, and *Integrity* (the CIA Triad).

[20] ISO/IEC 27000 documents the general terminology used in the cybersecurity domain

the vocabulary found with an additional set of standards through a **Terminological Validation** [21]. We promoted analysis of the terms found previously in the studies, looking for definitions in supplementary standards that are recognized by the cybersecurity community. Our objective is to first compare terms and definitions, and then evaluate the meaning of each term according to the context used. Our approach follows those adopted in [18, 15, 16], in which well-known and recognized standards support reference ontologies, providing an ontological analysis of the domain. Domain specialists of our team participate in this process, validating the meanings and the context of use regarding the terminology studied.

For the *Ontological Perspective*, we propose a **Framework for Classifying Ontologies**. This framework provides a clear baseline for classifying and comparing ontologies in the state-of-the-art. However, our initial proposal in [59] only considered three main ontology classifications [31, 36, 104]. From Guizzardi's classification of level of application [36], we take the notion that a Reference Ontology must support the implementation. Then, from Guarino's level of generality classification [31], we take the notion that the Ontology Grounding requires a Foundational Ontology. Even though the approach that uses the classifications [31, 36, 104] has proven itself to be useful for ontology characterization, we want to offer a more refined classification in our proposal. Therefore, we take into account additional classifications such as [103, 26, 25, 102] in this refined framework.

The framework includes a set of steps for ontology classification. The first step concerns the state of the art about ontology in research. Then, each subsequent step applies each of the selected well-known classifications [103, 26, 25, 102], providing a relation among them. We observe and analyze which aspects of each classification interfere with the other classifications in order to develop the framework. For instance, the limitations of the language used to implement an ontology interfere in many classifications with regard to: its application level (Operational Ontology), its axiomatization level (light-weight), and its formalization level (it cannot be highly formal if it is operational and light-weight). Following the classification framework, we can obtain a general picture of each ontology studied. Although each classification used presents its concerns, this orthogonal approach (based on several classifications) allows us to have a more comprehensive view of the ontologies studied in order to compare them.

5.1 The Cybersecurity Perspective Challenges

As the amount of cybersecurity standards and the vocabulary is vast, we are currently promoting a set of terminological surveys to help us complete the project required terminology. In doing this, we receive domain advice from a cybersecurity specialist of our research group, plus others who are members of the project consor-

[21] Note the vocabulary extension can be repeated as many times as necessary to achieve common sense among stakeholders

tium [22]. Meanwhile, we are also developing an API to help us administer all of this information which is stored in a NoSQL database. The objective is to facilitate communication among the stakeholders, providing a clean environment for discussions, feedback, and consensual agreement concerning the conceptualizations. We provide details of some of these results on the *Cybersecurity Perspective* in other publications [60, 87, 61] since they are out of the scope of this paper. Incidentally, since this is not a simple task, we present the main challenges we are facing in this process below.

Challenge 1: The high number of recognized cybersecurity standards and the different terminology definitions.

Although the ISO/IEC standards are our choice to be the terminological reference guide, there are several standards, glossaries, recommendations, and other guides that support the cybersecurity domain [56]. These documents usually present information that is consistent with each other, however, their applicability context may create misinterpretations. For instance, the meaning of the term "Risk" seemingly has a community consensus; however, it may still be controversial. While a manager can think about this concept from a general perspective ("*How much does it cost and what is the benefit?*"), a security engineer may think about the same term but from a specific perspective ("*What data we may lose and what is the impact?*") [70]. Both roles think they are talking about the same concept, but this is not true. The former is thinking about the "Estimation of the degree of exposure to a threat materializing on one or more assets causing damages to the Organization" from MAGERIT 3.0 [23], while the latter is talking about a standard perspective like the ISO/IEC 27000. In this case, both are definitions for the term "Risk" based on standards that are widely accepted by the cybersecurity community, but they mean different "*things*" regarding its semantics.

Challenge 2: The standards have different objectives (context, applicability, or viewpoint), so their use is multi-factorial.

Another issue occurs when stakeholders diverge about which of these documents to follow. There are situations in which the requirements are compulsory (by law) or must follow a country recommendation (requiring use of a particular standard), but their related definitions or viewpoint diverge from internal company doctrine. In the "Risk" example, while the use of MAGERIT 3.0 may be a requirement as a local standard, the ISO/IEC notion in a given project for a company may be the most suitable regarding security requirements [80]. In other words, using the concept associated with the term "Risk" either cannot be well-defined or a requirement will not be met, since having two different interpretations for the same concept is not acceptable when dealing with well-founded ontologies.

[22] Our research is part of a project to develop KGs (TKG and DTKGs) through a comprehensive solution within a project with Accenture LTD. The consortium also has research in partnership with other academic research centers.

[23] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Challenge 3: The standards drive the cybersecurity community to deal with the *Whats* but not with the *Hows*.

Besides the terminological misinterpretations, there are issues with relationships among concepts since the standards only define what the processes are but not how these processes may occur. This is the usual approach for standards since each organization must filter the best ways of implementing their internal policies with respect to their goals and doctrines on their own. Moreover, this is a problem that is aggravated in cybersecurity since this domain's standards usually deal with temporal and dynamic processes, tasks, or activities, reporting them to possible Task Ontologies or Application Ontologies [31].

In the **Terminological Validation**, we take into account the most frequently used cybersecurity standards accepted by this domain community. We selected standards from the International Organization for Standardization (ISO) [24], the International Electrotechnical Commission (IEC) [25], the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) [26] (including norms from the Consultative Committee for International Telegraphy and Telephony (CCITT)), the National Institute of Standards and Technology (NIST) [27], the North American Electric Reliability Corporation (NERC) [28], the Organization for the Advancement of Structured Information Standards (OASIS) [29], the Ministry of Foreign Affairs, European Union and Cooperation of Spain (MAEC) [30], the Spanish National Cybersecurity Institute (INCIBE) [31], and the MITRE Corporation [32]. In the next stage of our research, due to the great amount of generated data we plan to use standards from the Information Systems Audit and Control Association (ISACA) [33] and European Union Agency for Cybersecurity (ENISA) [34]. However, our proposal allows the inclusion of additional standards using the API that we have developed to facilitate our analysis.

5.2 The Ontological Perspective Challenges

Uschold and Gruninger [103] provide a classification consisting of highly informal ontologies, informally structured ontologies, semi-formal ontologies, and rigorously formal ontologies. This classification is consistent with the approach outlined by Guarino in [33]. However, the classification of ontologies based on their formalization level is not the only important aspect to be considered in the application of

[24] http://www.iso.org/iso/home.htm
[25] http://www.iec.ch/
[26] http://www.itu.int/ITU-T/
[27] http://csrc.nist.gov/
[28] https://www.nerc.com/
[29] http://www.oasis-open.org/
[30] http://www.exteriores.gob.es
[31] https://www.incibe.es/en
[32] https://www.mitre.org/
[33] http://www.isaca.org/Template
[34] https://www.enisa.europa.eu/

ontologies in Computer Science. The definition of what ontology is has evolved, disclosing the multidisciplinary aspect of ontologies. Gruber defines an ontology as "an explicit specification of a shared conceptualization" [29]. Borst defines as "a formal specification of a shared conceptualization" [13]. Studer et. al. defines as "a formal, explicit specification of a shared conceptualization" [92], which is a definition quite accepted by the Artificial Intelligence community. Afterward, according to the Ontology Engineering community, the multidisciplinary aspect of the knowledge expression through computational and ontological artifacts has been better clarified by Guarino in [30, 32] and Guizzardi in [36, 40, 37].

Different dimensions of ontology classification have emerged from this perception that ontologies transcend one single perspective. The classification based on the level of generality of the ontology (sometimes called knowledge kind) refers to a level of dependence on a specific point of view. Many proposals target this perspective, such as [92, 42, 19]. The most accepted classification of ontologies based on the level of generality is the proposal of Guarino [31], which complements the proposal of Mizoguchi and Ikeda [65]. Another widely accepted classification describes the Core Ontologies [104]. This results in five possible options for the classification based on the level of generality [31, 104]:

Foundational Ontologies (also known as High-level Ontologies or Upper Ontologies): express very general concepts and their relations like *things* and their properties, *events*, *time*, *space*, *relations* and their dependencies, whole/part relations (mereology). They are independent of a particular problem or domain.

Domain Ontologies: describe real-world domains of knowledge (e.g., the cybersecurity domain, the security domain, and others), by specializing the terms introduced in the foundational ontology.

Task Ontologies: describe a real-world tasks or activities to achieve a goal (like diagnosing or selling), also specializing the terms introduced in the foundational ontology.

Application Ontologies: describe aspects of both Domain Ontologies and Task Ontologies. They are often specializations of both the related ontologies (correspond to *roles* played while performing a certain activity, like replaceable unit or spare component).

Core Ontologies: are ontologies between the Foundational Ontology and the Domain Ontology (not as general as the Foundational Ontologies nor as specific as the Domain Ontologies).

Below, we present the main challenges we face when classifying ontologies.

Challenge 4: Not all ontologies have a foundational grounding.

Borrowing notions of Philosophy, Linguistics, Logic, and branches of science, Foundational Ontologies have emerged to provide conceptualizations for the most general aspects of knowledge and cognition and provide grounding for the more specific ontologies. Conceptualization like BWW [105], GFO/GOL [14, 43], DOLCE [12], UFO [34, 40] are examples of applied Foundational Ontologies. However, these ontologies are too general to allow their straight use as implementations themselves. Thus, they are the support for the design of Ontology-Driven Conceptual Languages

used to produce Domain, Task, or Application ontologies. Additionally, Foundational Ontologies can ground specific conceptualizations or provide ontological analysis for conceptual models. This statement is in line with the need for ontological grounding since the support of a Foundational Ontology avoids semantic interoperability problems in more specific ontologies [35]. Therefore, we advocate ontologies that must be evaluated according to their foundational grounding, separating ontologies that are driven by foundational ontologies (i.e., well-grounded) from ontologies without this support (i.e., not grounded).

Challenge 5: Not all implemented ontologies have a prior reference ontology (conceptual model) for knowledge representation.

Due to the multidisciplinary aspect, ontological artifacts have different roles under the umbrella of Ontological Engineering. Therefore, as a computational artifact, an ontology can be an "explicit and formal representation of a portion of reality for knowledge sharing", or it can be an "implementation of this representation for knowledge computational management". Thus, it is important to classify ontologies based on their application. Guizzardi classifies ontologies based on their application into two types: Operational Ontologies and Reference Ontologies [36]. A Reference Ontology should be a conceptualization that is constructed to make the best possible description of the domain with respect to a certain level of generality and point of view. An Operational Ontology is the actionable version of a Reference Ontology that uses the most appropriate language in order to guarantee desirable computational properties without compromising the previously defined ontological commitment [30, 32]. Therefore, there should be no operational ontology without the existence of data and its relationships as instances of previously well-defined concepts by a well-grounded reference ontology.

Challenge 6: It is difficult to evaluate the level of axiomatization and formalization from papers since the documents never provide enough details for that.

When implementing ontologies it is important to consider several engineering aspects. Similarly, in the software engineering process, the ontology engineering process involves making design decisions [4]. The platform of implementation, data volume and its sources, conceptual modeling, and the implementation language used influence these design decisions, often relinquishing axiomatization aspects in favor of the ability to conduct logical reasoning. Gomés-Peréz and Corcho [26] analyze the ontologies based on their axiomatization level (and considering the limitations of the language) in order to identify its computational limitations when a conceptualization becomes an implemented ontology (an Operational Ontology). They divide ontologies by considering the expressiveness of the language used into two aspects: Lightweight and Heavyweight ontologies. A bi-dimensional classification [25], based on [102] and [26], provides a link between the axiomatization and formal levels, focusing on the approach and expressiveness of the language. Figure 2 shows this classification.

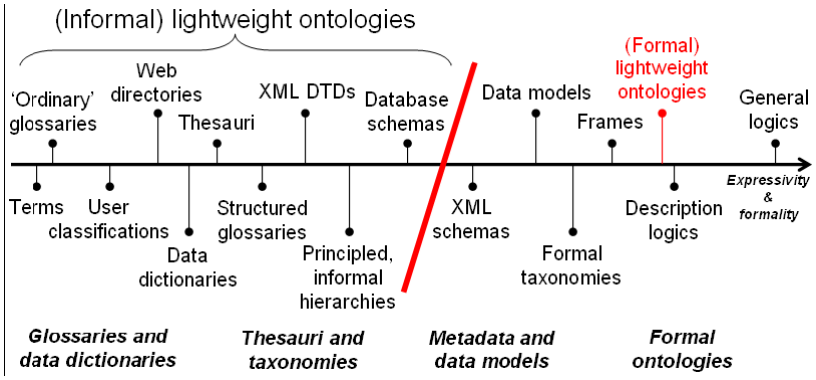


Fig. 2 Bidimensional classification according to [25].

There are other proposals that provide classifications for ontologies, but they are not as frequently used. For instance, there are works that provide a classification based on the nature of the real-world issue [52], the type of conceptualization structure [104], and the development method [89]. There are also bi-dimensional classifications [57, 27]. However, due to their limited use and to avoid increasing the complexity of the proposed framework, we do not use these additional classifications.

6 A Framework for Classifying Ontologies

Considering the ontologies studied and the conceptual characterization, we develop the **Framework for Classifying Ontologies**. The objective of the framework is to provide a homogeneous, clear, and well-established base to compare ontologies (Cybersecurity Ontologies) and their conceptualizations. The framework presents a five-step procedure to classify each ontology found in our previous literature search by using the considered classification levels. We point out that the characterization of an ontology using these classification levels is orthogonal since each classification can be executed in an encapsulated form, although there is a correlation among them. In other words, each classification level looks to the ontology with separation of concerns, but there are important aspects [35] and relations grounding these concerns. Besides, it is indispensable to consider that regarding functional spaces, families of orthogonal classification functions can be used to form a basis of comparison machine-understandable. Indeed, Section 5 clarifies the importance of a homogeneous basis of comparison to face the involved challenges in ontology interoperability in complex domains like cybersecurity. Section 7 shows how this bases of comparison can help in terms of ontological analysis for interoperability.

[35] Aspects in an ontological sense (essential properties).

6.1 Framework Description

In the process of identifying the characteristics of ontologies and their application within the cybersecurity domain, we aim to identify possible flaws of these ontologies both in terms of their definitions and implementations, as well as the consequences of semantic misinterpretations due to these deficiencies. Thus, we are evolving and consolidating the proposed framework for better ontology characterization based on the outcomes of our study.

Although the classification levels proposed are typically individual and independent, we present the framework through the five-step process as a sequence. Figure 3 shows the five steps for classifying ontologies that we recommend. We believe that a procedural description is more adequate to better express the different steps we conducted to reach the final characterization. Besides, this approach facilitates that the same procedure can be applied by other researchers. Moreover, in future work, it allows the operationalization of the procedure through a tool.

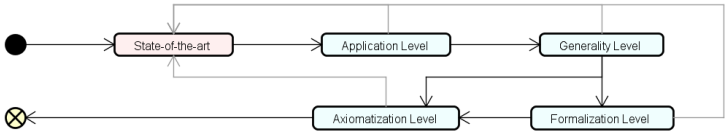


Fig. 3 Framework for Classifying Ontologies.

(1) State of the art: The first step shows that the process starts from a search for relevant information concerning the state-of-the-art ontologies covering a specific domain, which in our case is the cybersecurity domain. The process may refer to an ontology covering the entire domain, be composed of sub-ontologies each of which covers domain parts, or a more specific ontology in the domain. This can be performed through direct research with specialists, a survey, a literature mapping, or even a systematic literature review when reproducibility is required. Section 4 presents our approach. This is a cyclical process that must be repeated until the largest set of information is obtained. We use the documents summarized in Subsection 4.6 in this step of our research. Figure 4 presents the process in this step.

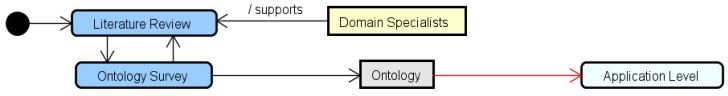


Fig. 4 Framework for classifying Ontologies - state-of-the-art step.

(2) Application Level: The second step provides the application level classification [36], which determines if the ontology documentation provides a *Reference Ontology*, an *Operational Ontology*, or both. The existence (or not) of a Reference Ontology

before its implementation depends on the choice of the design methodology used. Several methodologies drive the ontology design process. The SaBio methodology [4] requires the Reference Ontology to precede its Operational Ontology, but the most well-known and used methodology, the *Methontology* [20], does not. There is also a methodological domain-specific approach [71] that drives the cybersecurity ontology design according to a three-layer architecture (Upper, Mid-level, and Domain Ontologies). Thus, we also consider the adopted design methodology to be an aspect that is related to the analysis of the level of application, but not a classification itself. This process identifies which ontologies are well-defined and which are not. Figure 5 presents the process in this step.

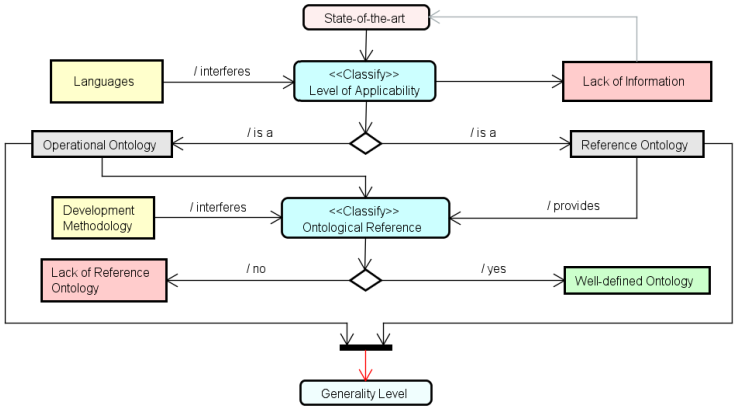


Fig. 5 Framework for classifying Ontologies - application level.

(3) Generality Level: The third step uses the generality level classification [31, 104]. This classifies the ontologies according to Guarino's proposal [31] into four types: *Foundational Ontologies* (also known as *High-level Ontologies*), *Domain Ontologies*, *Task Ontologies*, or *Application Ontologies*. It also classifies the ontologies according to Van Heijst's proposal [104] in *Core Ontologies*. Similarly, in this step, it is necessary to verify whether or not the ontologies have any ontological grounding through some *Foundational Ontology*. This process identifies which ontologies are well-grounded and which are not. Figure 6 presents the process in this step.

(4) Formalization Level: By using the information obtained in the first step, the fourth step makes a possible classification based on the ontology formalization following the bi-dimensional approach of [25]. This evaluation depends on the language used and its implementation (if it exists) as well as other ontology information. The analysis evaluates the distribution of the ontologies in a linear dimension from *Informal Ontologies* to *Formal Ontologies*. Then, the second dimension is relates to the classification proposed in [26], where the *Heavyweight Ontologies* correspond only to the ones from *Logic programming* to *General Logic* (this includes *First-order Logic*, *Higher-order Logic*, *Modal Logic*). Figure 7 presents the process in this step.

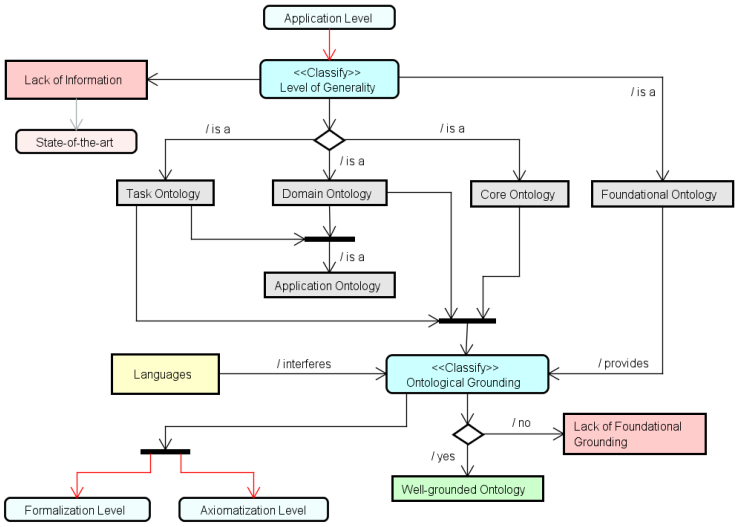


Fig. 6 Framework for classifying Ontologies - generality level.

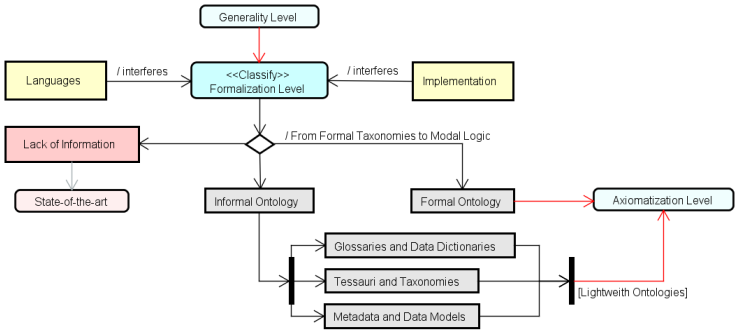


Fig. 7 Framework for classifying Ontologies - formality level.

(5) Axiomatization Level: The last step is directly related to the previous bi-dimensional classification made in Step 4. From the previous step, this classification groups the *Lightweight Ontologies* and the *Heavyweight Ontologies* based on their formalization level. The classification based on the ontology axiomatization level [26] evaluates the distribution of the ontologies in another linear dimension from *Lightweight Ontologies* to *Heavyweight Ontologies* based on the number of axioms (this value may be estimated). This evaluation also depends on the availability of information about the ontology, especially the language used and its implementation (if it exists). In other words, not all works provide details on the axiomatization for their proposed ontologies; in these cases, it is possible to do other state-of-the-art research for further details or just to identify the lack of information. Figure 8 presents the process in this step.

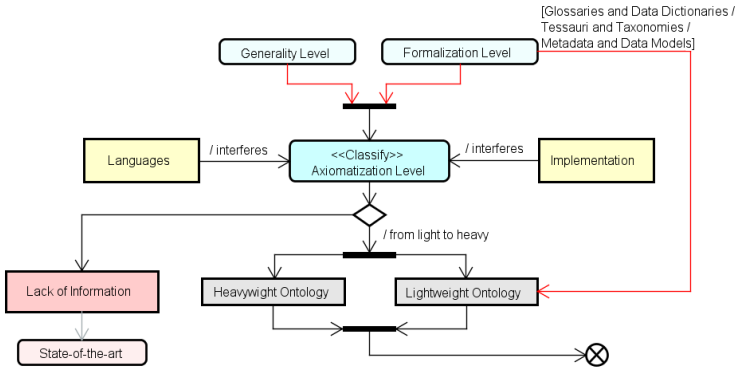


Fig. 8 Framework for classifying Ontologies - axiomatization level.

6.2 Applying the Framework

As previously mentioned, Section 4 presents the state-of-the-art step that we use to find information about the existing Cybersecurity Ontologies. CRATELO is one of the ontologies in which we apply the proposed framework. We now present how we were able to classify CRATELO as a *Well-grounded Operational Application Ontology*.

(1) State of the art: From our initial literature search (the pilot-study), we were able to find four papers [74, 76, 75, 6] describing CRATELO and two others extending it [75, 6]. Therefore, we use the information provided in these documents as the data source for the next steps in the framework. We also discuss the domain aspects involved in CRATELO with our cybersecurity team of specialists.

(2) Application Level: Based on the retrieved in step 1 of the framework, we identify that the authors implement CRATELO in OWL and SWRL with Protègè. Therefore, the appropriate classification based on its Application Level for CRATELO is *Operational Ontology*. Then, we verify if there are any prior Reference Ontology supporting the implementation. In this process, we identify that there is no *reference conceptual model* (Reference Ontology) supporting the *operational conceptual model* of CRATELO implemented in Protègè. We also take in account the aspects of the ontology that interfere in this classification, like the methodology used in its development, which includes design decisions (the language chosen). Moreover, we analyze the relationship between other considered classifications and the application level in order to corroborate the classification. In detail:

The language: Even though Protègè provides a graphical representation of the ontology, this model is not a reference ontology because of the language used (OWL). Instead, this is an *operational conceptual model* (an implementation). OWL provides lightweight conceptualizations (regarding the *Axiomatization Level*), and reference ontologies are necessarily heavyweight (i.e., they must consider all possible sets of constraints required to represent the best real-

world approximation of the domain). This notion is well explained in [25] (see Figure 2).

The methodology: The lack of a prior reference ontology denotes a methodological issue because we consider CRATELO to be *Well-grounded* (regarding the generalization level analysis). Since CRATELO is an ontology that is supported by DOLCE-Spray, we need to look at the DOLCE-Spray (and DOLCE) analysis to keep going with the CRATELO classification. DOLCE-Spray is also an Operational Ontology (in terms of its Application Level) because it is an implementation in OWL-Lite. Since DOLCE-Spray is a lightweight implementation of DOLCE, DOLCE is its prior reference ontology (and Foundational Ontology based on its generality level classification). With regard to the language, DOLCE is an ontology that is formally specified in first-order logic (FOL) – heavyweight (considering its expressiveness based on the *Axiomatization Level*). In other words, CRATELO is well-grounded because it is an ontology that is supported by DOLCE-Spray. However, by contrast to DOLCE-Spray, which has DOLCE as a reference, CRATELO has no reference ontology counterpart (for instance, founded in DOLCE).

(3) Generality Level: Among the papers presenting CRATELO, the work in [74] depicts part of the ontology (a CRATELO sub-ontology) that deals with tasks, activities, and processes as well as domain concepts; therefore, it is an Application Ontology. Guarino's classification of *Application Ontology* is the one that presents aspects of both Task and Domain Ontologies. The other documents [74, 76, 75, 6] (from Step 1) as well as the CRATELO extensions [75, 6] only present Domain Ontologies. Therefore, we use the most comprehensive classification for CRATELO (considering all of its sub-ontologies) to classify it as an *Application Ontology* based on its generality level. We classify CRATELO as a *Well-grounded Ontology* because it is an ontology grounded on DOLCE-Spray.

(4) Formalization Level: Following the framework steps, we again focus on the language used and the implementation itself to classify CRATELO in the group of *Formal Ontologies* and the subgroup of *Lightweight Ontologies* based on the bi-dimensional classification proposed in [25] (see Figure 2).

(5) Axiomatization Level: Finally, the last step of the framework classifies CRATELO ontology according to the proposal in [26]. This classification is divided only into *Heavyweight Ontologies* or *Lightweight Ontologies*, depending on the number of axioms annotated in the conceptualization. In this case, we classify CRATELO as a *Lightweight Ontology*. However, CRATELO is also in the group of *Formal Ontologies* classified in the previous step of the framework, which can comprise ontologies that fit into any of these levels of axiomatization. Note that the previous classification puts CRATELO in the subgroup of *Formal Ontologies* called *Lightweight Ontologies*, which has the same naming in a different classification. This similarity in terminology is not by chance. Instead, it occurs because the proposal [25] also considers the axiomatization level classification [26] as a parameter of analysis. The framework considers this last classification again even though it is already present in the previous Step 4 because there are research cases where not all documents found have enough information to provide the previous classification as we made with CRATELO. In other words, the framework allows

an axiomatization level classification in this final step even when it is not possible to have all of the details to provide a good classification in Step 4.

Using the framework, we classify all of the ontologies that we studied from our state-of-the-art research. The main point of this strategy focuses on the possible relationships between these ontologies (i.e., grounding, specializations, generalizations, intersections, and overlapping). Besides the design decisions taken, the language used, and the methodological approach adopted regarding the ontology itself, we also analyze the following:

- all ontological grounding, both in the sense of the domain and its concepts;
- the possible unions and intersections among the ontologies, considering both the domain and its concepts;
- the bottom-up approach, looking for more general conceptualizations;
- the top-down approach, looking for more specific conceptualizations.

In this classification process, the relations among the studied ontologies are as important as the inside-domain conceptualization (concerning domain terminology and its definitions). In other words, the Ontology Engineering Process and the design decisions taken participate (as a whole) in the results of a conceptualization as much as the conceptualization itself. This is where an orthogonal and well-founded classification framework applied to the ontologies allows us to identify possible inconsistencies, misinterpretations, and misunderstandings.

For instance, we classify COoVR as follows: a *Well-grounded Reference Ontology* based on its application level; a *Domain Ontology* based on its granularity level; a *Formal Ontology* (*General Logic*) based on its formalization level; and a *Heavyweight Ontology* based on its axiomatization level. The COoVR is about the domain of *Value* and *Risk* in general, which are important notions that are also presented in the security domain (as well many others). The intersection of domains is an important issue not only in terms of interoperability but also regarding reusability (FAIR principles). Therefore, our approach not only observes more specific ontologies (sub-ontologies) in the domain of cybersecurity, but it also observes more general ontologies that may support the concepts of this domain. Indeed, the authors of COoVR are clear about the possible of it uses in many domains, including when they discuss the security domain-related flaws of their ontology (see [84], p. 133).

The SECCO (which is part of CRATELO) is another example of the same approach: “A middle-level ontology of security can be possibly extended beyond SECCO: in this respect, the key contribution of this module doesn’t rely on the coverage (or ‘concept density’) of security primitives but on the formalization driven by a top-level ontology” [74]. Note that the authors of SECCO are also aware of a future need for its extension to include concepts of *Risk* (see [74], p. 60). Therefore, we classify SECCO as: a *Well-grounded Operational Ontology* based on to its application level; a *Core Ontology* based on its granularity level; a *Formal Ontology* (*Lightweight*) based on its formalization level; and a *Lightweight Ontology* based on its axiomatization level.

6.3 Summary of the Framework Results

Finally, we propose a template form to synthesize the results obtained for each ontology from the review extraction and the application of the framework. We document each of the ontologies (and their sub-ontologies) that we found by filling out this template and summarizing our impressions. Table 4 shows the document filled with the CRATELO ontology classification after the framework application and summarization.

Table 6 The proposed framework template for ontology classification - CRATELO.

CRATELO Ontology	
The CRATELO [74, 76] is a three-layer ontology [71] proposal for the domain of cybersecurity (Domain Ontology). It is grounded on a Foundational Ontology named DOLCE-spray [73], a simplification of the DOLCE ontology. The CRATELO ontology also includes the Security Core Ontology (SECCO) and the Domain Ontology of cyber operations (OSCO). It is a well-grounded ontology implemented with OWL and SWRL with Protègè. The CRATELO has some extensions described in [75, 6].	
Application level	
Reference Ontology ☐	Operational Ontology ☒ OWL-lite Protègè
Implementation	
Well-defined ☐	Imprecise ☒
In the papers found, we are not able to identify any Reference Ontology. As we know, our research string is limited, and because it is an initial search, this additional information can modify this evaluation in further literature searches. We are considering the ontology presentation through OWL as implementation, i.e., an Operational Ontology.	
Generality level	
Foundational Ontology ☐	
Core Ontology ☐	Domain Ontology ☐
Task Ontology ☐	Application Ontology ☒
Since CRATELO is composed by many sub-ontologies (Domain Ontologies or Task Ontologies), we classified the full CRATELO as an Application Ontology.	
Grounding	
Well-grounded ☒	Not grounded ☐
Foundational Ontology: DOLCE-spray [73]	
DOLCE-spray is an OWL-lite version of DOLCE [12, 63, 64]	
Formalization level	
Classifiable ☒	*Unclassifiable* ☐
Glossary and Data dictionaries Terms ☐ Glossaries ☐ Ad-hoc Hierarchies ☐ Data Dictionaries ☐	**Metadata and Data models** XML Schemas ☐ Data Models ☐
Thesauri and Taxonomies Thesauri ☐ Structured Glossaries ☐ XML, DTDs ☐ Informal Hierarchies ☐ DB Schemas ☐	**Formal ontologies** Formal Taxonomies ☐ Lightweight Ontologies ☒ Logic Programming ☐ Description Logic ☐ General Logic ☐
Informal ——▲—— Formal	
Axiomatization level	
Classifiable ☒	*Unclassifiable* ☐
Lightweight ——▲—— Heavyweight	
Number of axioms: unknown	
We estimated the axiomatization based on the details provided in the papers we found.	

The framework helps to describe the ontology and its classification individually, but this is not the main result that can be extracted. From the ontological perspective, it is possible to establish relations among the studied ontologies. For instance, if one ontology is a sub-ontology of another; if one reference ontology provides one or more (different) implementation versions (operational ontologies); which ontologies use the same (or similar) foundational ontology; which are the ontologies overlapping the domain (or domain parts); among others. From the domain perspective, the terminological verification and validation provide the standardization support and context applied to the ontologies that allow knowing how the specialists in-depth use the conceptualizations. Furthermore, by bringing these perspectives together, we can produce outcomes such as those shown in Figure 9 which presents the concept of *Risk* cross-analysis. We discuss the details of this analysis in the next section.

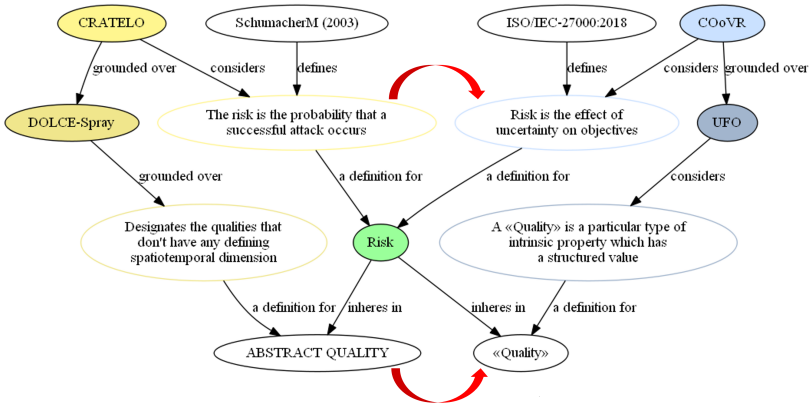


Fig. 9 The concept of *Risk* concept cross-analysis as an outcome of the ontology characterization framework.

7 Cross-analysis of the Two Perspectives

Section 6 describes the refined **Framework for Classifying Ontologies** according to the *Ontological Perspective* that we extended from [59]; in [59, 61, 87], we presented the Cybersecurity Terminological Validation from the *Cybersecurity Perspective*. In light of these two perspectives, in this section, we present a comparative analysis of the results obtained. The goal of this Cross-analysis is to define a strong and systematic base of comparison to support interoperability among conceptualizations. During the Cross-analysis, we can identify if the ontologies are well-grounded, their ontological commitment, and other specific characteristics. It is then necessary to provide an ontological analysis for the ontologies that are not well-grounded by using a Foundational Ontology. The objective of this ontological analysis is not to criticize the ontology itself. Instead, the goal is to identify patterns and anti-patterns in light of a Foundational Ontology and consequently provide the necessary basis for the next step of the interoperability process.

The search for patterns helps us to systematize behaviors and actions. According to the OED definition, a Pattern is "the regular way in which something happens or is done"[36]. In Computer Science, the GoF [22] provides the notion of *Design Patterns*, helping modelers and programmers in understanding and systematizing their work. In the conceptual modeling best practices, the use of design patterns is widespread. However, not all of the regular ways of doing something are correct. Indeed, being humans that we are, we also systematize mistakes and misinterpretations. When this happens in conceptual models, modelers can experiment with a cognitive model misinterpretation or even future unexpected behavior of data (when they have models implemented). This kind of modeling issue is known as a *Design Anti-pattern*. According to [83] "ontological anti-patterns are error-problem modeling structures that can create a deviation between the possible and the intended interpretations of an ontology." In [38], the perception that "recurrent configurations that potentially make a particular model accept as valid some instances that are not intended (or, in other words, that are not compatible with its ontological commitment)" are considered *Ontological Anti-Patterns*. Therefore, the possible anti-patterns found during an ontological analysis help us to fill misinterpretation gaps about a concept and its relations as well as help us to know their unpredicted consequences.

For instance, let's take the notion `Risk` from the SECCO ontology, which is part of CRATELO. We compare its notion of `Risk` with other approaches. Then, we analyze how the ontology classification framework will help us to give meaning to these conceptualizations and evaluate differences, similarities, and approximations. Our goal is to verify the possibility (or impossibility) of interoperability among these ontologies.

We classify SECCO as an *Operational Core (Lightweight) Formal Ontology* that is well-grounded on DOLCE-Spray for the Security Domain in general (Subsection 6.2). This classification is also loaded in the NoSQL database that we developed to provide future reasoning capabilities. From this analysis, it is possible to establish a benchmark based on classification primitives, i.e., establish the ontological commitment [30]. The language of representation is OWL-Lite, and the SECCO formalizes *Risk* as "a `DEFENSIVE_OPERATION` needed to run a `RISK_ASSESSEMENT` of the `RISK` associated to a sequence of `MISSION_TASKs` (datatype properties can be used to represent a `RISK` as a parameterization of the expected losses, probabilities of attack, etc.)" [74]. The relation `isQualityOf` [37] and the `hasParticipant` [38] used with this perspective is from DOLCE-Spray.

Since the SECCO ontology conceptualizes the security domain in general, it can predicate a broad spectrum of things. It defines *Risk* as follows: "The risk is the probability that a successful attack occurs" [86]. Therefore, this notion is more general and concerns anything that requires being secure, not only cybersecurity. We must point out that: (i) `Risk` is quantifiable and allows comparisons; (ii) it does not exist by itself, and depends on another "*thing*" to exist (*the thing at risk*); and (iii) it

[36] https://www.oxfordlearnersdictionaries.com/definition/english/pattern_1

[37] $RISK \sqsupseteq ABST\_QUALITY \sqcap \forall\ isQualityOf.MISSION\_TASK$

[38] $RISK\_ASSESSMENT \sqsupseteq ACTION \sqcap \exists\ hasParticipant.RISK$

should happen through some *Event*[39], denoted here by the notion of *Attack*, which is also used in a general connotation. Therefore, the ontological grounding provided by DOLCE-Spray conceptualizes *Risk* as a *quality*.

From the terminological validation (*Cybersecurity Perspective*), most definitions provided by standards mention *Risk* as a "measure", a "possibility of harm", a "likelihood", or even a "level of impact", although the contexts and object to which *Risk* applies to vary. This means that an ontological analysis is required for each ontology that we want to interoperate with. The objective is to do the following:

1. verify if the *Risk* concept is the same at the ontological level;
2. identify the concepts in which the *Risk* is applicable ("*the thing at risk*") , including its relations;
3. verify if the context of use for both the "*the thing at risk*" and the *Risk* itself.

Therefore, we propose the following competence questions:

Question 1 Is the *Risk* concept interoperable between SECCO and COoVR?

We classify the COoVR as a *Reference Domain Formal Ontology* for the Domain of Risks and Values in general (Subsection 6.2), and which main concepts can be extended for the Security Domain. Similarly, in SECCO, the concept of *Risk* according to the COoVR has a qualitative perspective, i.e., it is a *moment* that is expressed according to a value space [34, 39]. The *Risk* depends on another concept to exist; in this case, `Risk` is a <<*Quality*>> [40] of the `Risk Assessment`. The `Risk Assessment` is a relational element (<<*Relator*>> [41]) that mediates the agent that is responsible for the judgment (deemed `Risk Assessor`) and the target of the judgment. In this case, the judgments made for *objects* are labeled as `Object Risk Assessment` and `Object at Risk`. Judgments on events are `Experience Risk Assessment` deemed and involve entityRisk Experience [84].

The notion of *quality* from DOLCE and UFO are similar, so the *Risk* concept is aligned with the two ontologies. It is also worth mentioning that the concept of *Risk Assessment* in DOLCE-SPRAY is treated as an ACTION instead of a relational moment (<<*Relator*>>) as in UFO. This occurs because the notion of *Event* from DOLCE and UFO are slightly different. While DOLCE puts an *Event* at the level of *moments*, UFO treats this concept as manifestations of dispositions. This difference has other implications that we do not mention here since they are out of the scope of this publication. In any case, the concept of *Risk* in the SECCO and COoVR ontologies are interoperable depending on the concepts in which the *Risk* is applicable.

Question 2 Is the *Risk* concept interoperable between SECCO and the Ontology of ISO/IEC 27005?

Unlike SECCO, the Ontology of ISO/IEC 27005 lacks the fundamental concepts to identify philosophical differences between the represented concepts. Therefore,

[39] Here we are considering the ontological notion of Event as a *Perdurant* from DOLCE [12].

[40] The stereotype for UFO intrinsic moments for the OntoUML [34] language.

[41] The stereotype for UFO relational moments for the OntoUML [34] language.

it is necessary to provide an ontological analysis of this domain ontology by using some foundational ontology as grounding. We chose UFO for this purpose because it successfully supports studies for ontological analysis, such as [15, 21, 2]. Besides, UFO grounds the COoVR (one of the ontologies used in this case of study). Figure 10 shows the Ontology of ISO/IEC 27005 and its ontological analysis in light of UFO and presented as an OntoUML diagram [42]. Figure 10(a) shows the original proposal using proper language notation, while Figure 10(b) shows our analyzed version using the OntoUML notation.

In this case, through the ontological analysis of Figure 10(b), we can identify that the `Risk` is a role (<<*RoleMixin*>>) in this ontology. The `Risk` is a role that can be assumed by a `Consequence` or `Threat` (both <<*Event*>>) when an instance of one of them *leads on* `Vulnerabilities` (which is a <<*material*>> relation between them). This is quite different from the SECCO and COoVR *Risk* notion as a quality (<<*Quality*>>) of *Risk Assessment*. In fact, the Ontology of ISO/IEC 27005 defines `Risk` as "a class represents an effect of uncertainty on objectives" [1]. In this ontology, the concept of *Risk* gets closer to the notion of *Risk Experience* (`Risk Experience`) in COoVR. For all of these reasons, the concept of *Risk*, as it is defined in the Ontology of ISO/IEC 27005, is not interoperable with the concept of *Risk* in SECCO.

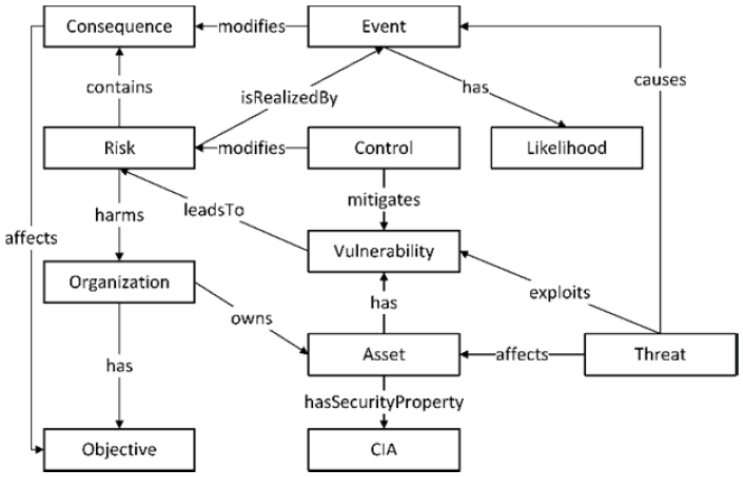
Question 3 Is the *Risk* concept interoperable between SECCO and Mulval?

Using the same approach, we look for any kind of foundation ontology that supports MulVAL [78]. MulVal is an efficient tool for the implementation and reasoning of AGs. However, the MulVal tool lacks a strong ontological grounding despite being based on well-known taxonomies and standards. This occurs because these taxonomies and standards are not grounded on any foundational ontology. As a result, in a KG instance implementation, any change in the MulVal tool setup produces different perspectives (commitments) of the very same concept representation. In other words, each instance of a KG may conceptualize the data associated with the concept *Risk* taking into account different viewpoints, depending on its setup. Thus, each KG instance must require its individual ontological analysis, making the integration process costly. Therefore, for this integration process, the MulVAL will be discarded as an ontology to be interoperable with SECCO.

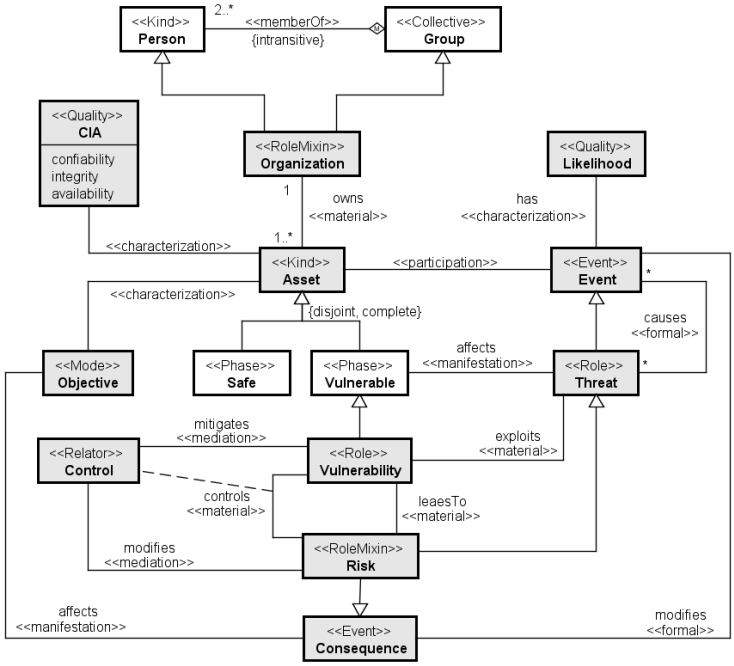
Question 4 Is the *Risk* concept interoperable between SECCO and other ontologies?

For a possible integration with other ontologies, similar to the Operational Ontologies that we found, a common approach is the conceptual matching comparison in the ABox, verifying formal characteristics as we describe in Section 2. However, there are no guarantees that similar formalization provides similar meaning without misinterpretations. This occurs because this kind of analysis does not consider the Ontological Level [30], using syntactical analysis, meta-language analysis, and structural language comparison, which are neutral perspectives. In other words, a foundational grounding is required even for the best formalization approaches. Since

[42] OntoUML specification at https://ontouml.readthedocs.io/en/latest/ and https://github.com/OntoUML



(a) Original fragment [1].



(b) Ontological Analysis on UFO.

Fig. 10 Ontological Analysis of the Ontology of ISO/IEC 27005 [1].

most of the ontologies lack grounding, an ontological analysis is required. The goal of the Cross-analysis presented is to support this process and fill this gap.

8 Impact on Ontology Engineering

This case-of-study shows that the effort required to reach semantic understandability among ontologies goes beyond structural aspects. The entire umbrella of Ontology Engineering process is affected. Looking at the Ontology Engineering process and considering the quest to fulfill the FAIR principles, the Cross-analysis seems to confirm the level of complexity that the Ontology Interoperability process has, especially in domains like cybersecurity.

We provide a comparative study taking into account only one concept (*Risk*) in four of the ontologies that we found. Although our analysis deals with only one concept and its close relationships, the notion of *Risk* is complex in itself. Using this example, we are dealing with definitions from diverse contexts, all of which are well-supported by known cybersecurity standards. Indeed, *Risk* and its surrounding conceptualization involve different approaches between the communities of Ontology Engineers and Domain Specialists. Moreover, according to Oltramari in [72], "At the same time, neither practitioners nor ontologists pay comparable attention to the concepts traditionally associated with risk, such as probability or likelihood of an adverse event, and the cost of consequences or impact of the event. Such concepts, which are canonical in most definitions inspired by traditional definitions of risk, are mentioned very infrequently in discourses of practitioners and with only moderate frequency by ontologists". This denotes the importance of analyzing a concept using a broad approach, either looking for more general conceptualizations or for more specific ones. Furthermore, it is necessary to analyze possible intersections and unions of the definitions taken and according to their contexts. The main problem basically results in issues of conceptual ambiguities caused by the lack of an ontological foundation combined with the complexity of the domain itself.

In this scenario, the most significant information we extract is the lack of foundational grounding in the cybersecurity ontologies that we found. In the first round of search, only four papers mention a foundational grounding, and all of them are related to the CRATELO proposal [74, 76, 75, 6]. In the second round of search, the well-grounded ontology extracted is one of those that we manually add, the COoVR [84]. In the Cross-analysis presented in Section 7, we demonstrate the importance of a strong conceptual basis when the support of a Foundational Ontology avoids semantic interoperability problems in Domain Ontologies [35]. Therefore, the better developed the ontologies are, the less effort will be required to promote interoperability among them.

Besides the lack of grounding that we detect, most papers mentioning Operational Ontologies have been implemented without a prior reference ontology (80% have no prior Reference Ontology). In contrast, the proposals of Reference Ontologies are not implemented (20% of the total), and there was no justification provided. Only the Ontology of Cybersecurity Operational Information [98, 99, 97, 96], CoCoa [77], OVM [106], and CVO & CIO - CIA System [94] proposals provide an Operational

Ontology that is supported by a prior Reference Ontology. This notion that operational ontologies and their implementations require the support of a prior reference ontology is well-established in [36]. Therefore, Ontology Engineers must regard the importance of choices made in their design decisions, like languages and implementation platforms. The proposed framework takes into account these choices denoting their influence on classifying ontologies.

The main cause of these problems comes from the ontology design methodologies adopted. In other words, these methodologies do not perceive that the best practices already established in the Software Engineering Process are an experience that be used as best practices of the Ontology Engineering Process. The SaBio [4] methodology is the only one we know that has a proposal to fill those gaps. Based on that, we suggest that Ontology Engineers must take best-practice actions such as following:

- Maintain efficient and high quality communication with Domain Expert stakeholders;
- Use a methodology that drives the process by using Reference Ontologies before the implementation of Operational Ontologies;
- Use a well-defined ontological grounding for the design process Reference Ontologies;
- Adequately justify the reasons for not implementing a Reference Ontology by either justifying that it is a project requirement itself or explaining why the implementation was not viable. This is a methodological question that is yet to be answered.

Realizing that many of the issues mentioned above are related to the different views taken by ontology engineers and domain specialists (in this case, cybersecurity specialists), we propose a REST-API presented in [61] to help stakeholders consolidate the data and their viewpoints. This kind of solution is intended to support the ontological analysis of domain ontologies. Besides, it has the potential to become a complete ontological analysis support tool that is able to provide reasoning and present data through a friendly interface (frontend). This sounds like a useful secondary contribution with regard to the Ontology Engineering process in general and a future work proposal.

9 Conclusions

Our research deals with the quest that involves implementing the FAIR principles. Among these, is assessing the ontology-based conceptual interoperability. Our final goal is to provide a solution that mainly fills the research gaps that the industry still has open. Enterprises require interoperability for their data, so they have professional tools and specialized personal. However, they do not have a definitive solution that links their resources to the ontology-based conceptual approaches. Academies have great ontology-based solutions, but they are still not applicable enough. Since this research is part of a multidisciplinary consortium composed of industry and academic teams, we believe future results are promising.

We promote initial state-of-the-art research studies [60, 59]. As a result, we depict the particularities of the found ontologies, like those we mention in Section 5. We also use our preliminary state of the art to identify the vocabulary used by the ontologies covering the Cybersecurity Domain through a survey [87]. We are planning other survey cycles to include all of the vocabulary and definitions. Our objective is to cover the most commonly used and known cybersecurity standards. At the same time, we are developing a backend solution [61] to deal with all of the data about the cybersecurity ontologies recovered from the state of the art and its vocabulary-related surveys. The goal is to facilitate the cross-analysis process, provide dynamic data access and a flexible solution for ontology classification based on the presented framework and easy domain conceptual definition.

We will validate this research by using several commercial applications of Accenture LTD. We aim to use several contexts such as insurance, prioritization in taking actions, cyber investment rationale, and management of alerts. We plan to evaluate, in these scenarios, whether or not the framework will achieve interoperability and to provide well-grounded KGs implementations by focusing on two main points:

1. if it can help the stakeholders in identifying and classifying related ontologies on these commercial applications;
2. if it provides support for their cross-analysis.

At this point in our research, it is not possible to provide quantified information. Measurements such as time estimation, human resource effort, financial or other numerical details require more validation time and effort. Given our initial state-of-the-art results and the subsequent steps already implemented, we are aware that this is not a low-cost effort. Therefore, this is another issue that can enhance the research, since each mistake or misunderstanding that is not avoided in an interoperability process in complex domains can involve untold losses. Moreover, we consider this kind of measurement and quality evaluation to be an opportunity for future research work. One of the possibilities is to provide measurements and quality evaluations to compare manual ontological analysis with the process done using our proposal.

In conclusion, in this work, we present a **Framework for Classifying Ontologies** as the first contribution. We have presented our proposal using the cybersecurity ontologies found in the state of the art. We have presented some findings that we were able to retrieve as well as an example of the kind of questions that we can answer during the **Cross-analysis of the Two Perspectives** (the *Ontological and the Domain Perspectives*). The cross-analysis is our second contribution; we have only shown a fraction of the results that are possible with our approach. We are aware that we have only worked with a single (*Risk*) concept and its surrounding notions; however, we believe that it is sufficient to demonstrate the complexity of the interoperability process. We have also discussed the impact of our findings on Ontology Engineering, highlighting challenges involved in the process. We have also suggested best practices for Cybersecurity Ontologies implementation that are useful for ontology design and development in general. This research is also the basis for the definition and design of a definitive and well-grounded architecture for KG creation, update, and manipulation.

Acknowledgements This work has been developed with the financial support of the Accenture LTD (Accenture Labs, Tel Aviv, Israel) and Spanish State Research Agency under the projects "Digital Knowledge Graph - Adaptable Analytics API" and MICIN/AEI/ 10.13039/501100011033 and co-financed with ERDF and the European Union NextGenerationEU/PRTR.

References

1. Agrawal V (2016) Towards the ontology of iso/iec 27005:2011 risk management standard. In: HAISA
2. Almeida JPA, Guizzardi G (2013) An ontological analysis of the notion of community in the rm-odp enterprise language. Computer Standards & Interfaces 35(3):257–268
3. Almeida JPA, Guizzardi G, Sales TP, Falbo RA (2019) gUFO: A Lightweight Implementation of the Unified Foundational Ontology (UFO). Tech. Rep. Version 1, Federal University of Espirito Santo, URL https://nemo-ufes.github.io/gufo/
4. de Almeida Falbo R (2014) Sabio: Systematic approach for building ontologies. In: Guizzardi G, Pastor O, Wand Y, de Cesare S, Gailly F, Lycett M, Partridge C (eds) Proceedings of the 1st Joint Workshop ONTO.COM/ODISE on Ontologies in Conceptual Modeling and Information Systems Engineering, CEUR-WS.org, CEUR Workshop Proceedings, vol 1301
5. Babiceanu RF, Seker R (2017) Cybersecurity and resilience modelling for software-defined networks-based manufacturing applications. Studies in Computational Intelligence 694:167–176, DOI 10.1007/978-3-319-51100-9_15
6. Ben-Asher N, Oltramari A, Erbacher RF, Gonzalez C (2015) Ontology-based adaptive systems of cyber defense. In: STIDS, pp 34–41
7. Benevides AB, Guizzardi G (2009) A model-based tool for conceptual modeling and domain ontology engineering in ontouml. Enterprise Information Systems pp 528–538
8. Bergner S, Lechner U (2017) Cybersecurity ontology for critical infrastructures. In: KEOD, pp 80–85
9. Bizer C, Heath T, Berners-Lee T (2011) Linked data: The story so far. In: Semantic services, interoperability and web applications: emerging concepts, IGI Global, pp 205–227
10. Blanco C, Lasheras J, Valencia-García R, Fernández-Medina E, Toval A, Piattini M (2008) A systematic review and comparison of security ontologies. In: 3th International Conference on Availability, Reliability and Security, IEEE, pp 813–820
11. Booth H, Turner C (2016) Vulnerability description ontology (vdo). A Framework for Characterizing Vulnerabilities NIST
12. Borgo S, Masolo C (2010) Ontological Foundations of DOLCE, Springer Netherlands, Dordrecht, pp 279–295
13. Borst WN (1997) Construction of Engineering Ontologies for Knowledge Sharing and Reuse. CTIT, Centre for Telematics and Information Technology

14. Degen W, Heller B, Herre H, Smith B (2001) Gol: toward an axiomatized upper-level ontology. In: Proceedings of the international conference on Formal Ontology in Information Systems-Volume 2001, pp 34–46
15. Duarte BB, Souza VES, de Castro Leal AL, de Almeida Falbo R, Guizzardi G, Guizzardi RS (2016) Towards an ontology of requirements at runtime. In: FOIS, pp 255–268
16. Duarte BB, Falbo RA, Guizzardi G, Guizzardi RS, Souza VE (2018) Towards an ontology of software defects, errors and failures. In: International Conference on Conceptual Modeling, Springer, pp 349–362
17. Elnagdy SA, Qiu M, Gai K (2016) Cyber incident classifications using ontology-based knowledge representation for cybersecurity insurance in financial industry. In: 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, pp 301–306
18. Falbo R, Bertollo G (2009) A software process ontology as a common vocabulary about software processes. Int J Bus Process Integr Manag 4:239–250
19. Fensel D (2001) Ontologies. In: Ontologies, Springer, pp 11–18
20. Fernández-López M, Gómez-Pérez A, Juristo N (1997) Methontology: From ontological art towards ontological engineering. In: Proceedings of the Ontological Engineering AAAI-97 Spring Symposium Series, American Asociation for Artificial Intelligence
21. Gailly F, Geerts G, Poels G (2009) Ontological reengineering of the rea-eo using ufo. In: International Workshop on Ontology-Driven Software Engineering
22. Gamma E (1995) Design patterns: elements of reusable object-oriented software. Pearson Education India
23. Gasmi H, Laval J, Bouras A (2019) Cold-start cybersecurity ontology population using information extraction with lstm. In: 2019 International Conference on Cyber Security for Emerging Technologies (CSET), pp 1–6, DOI 10.1109/CSET.2019.8904905
24. Giaretta P, Guarino N (1995) Ontologies and knowledge bases towards a terminological clarification. Towards very large knowledge bases: knowledge building & knowledge sharing 25:32
25. Giunchiglia F, Zaihrayeu I (2007) Lightweight ontologies. Tech. rep., University of Trento
26. Gómez-Pérez A, Corcho O (2002) Ontology languages for the semantic web. IEEE Intelligent systems 17(1):54–60
27. Gomez-Perez A, Fernández-López M, Corcho O (2004) Ontological Engineering: With Examples from the Areas of Knowledge Management, E-Commerce and the Semantic Web. Springer Verlag
28. Grégio A, Bonacin R, Nabuco O, Afonso VM, De Geus PL, Jino M (2014) Ontology for malware behavior: A core model proposal. In: 2014 IEEE 23rd International WETICE Conference, IEEE, pp 453–458
29. Gruber TR, et al. (1993) A translation approach to portable ontology specifications. Knowledge acquisition 5(2):199–220
30. Guarino N (1994) The ontological level. Philosophy and the Cognitive Sciences
31. Guarino N (1998) Formal Ontology in Information Systems. In: Proceedings of the 1st International Conference, IOS Press, Trento, Italy, pp 6–8

32. Guarino N (2009) The ontological level: Revisiting 30 years of knowledge representation. Conceptual modeling: Foundations and applications pp 52–67
33. Guarino N, Poli R (1995) The role of formal ontology in the information technnology. International journal of human-computer studies 43(5-6):623–965
34. Guizzardi G (2005) Ontological Foundations for Structural Conceptual Models. CTIT, Centre for Telematics and Information Technology
35. Guizzardi G (2006) The role of foundational ontology for conceptual modeling and domain ontology representation, keynote paper. In: 7th International Baltic Conference on Databases and Information Systems (DB&IS), Vilnius, IEEE Press
36. Guizzardi G (2007) On ontology, ontologies, conceptualizations, modeling languages, and (meta) models. Frontiers in artificial intelligence and applications 155:18
37. Guizzardi G (2013) Ontology-based evaluation and design of visual conceptual modeling languages. In: Domain engineering, Springer, pp 317–347
38. Guizzardi G (2014) Ontological patterns, anti-patterns and pattern languages for next-generation conceptual modeling. In: International Conference on Conceptual Modeling, Springer, pp 13–27
39. Guizzardi G, Zamborlini V (2014) Using a trope-based foundational ontology for bridging different areas of concern in ontology-driven conceptual modeling. Science of Computer Programming 96:417–443
40. Guizzardi G, Pires LF, Van Sinderen M (2005) An ontology-based approach for evaluating the domain appropriateness and comprehensibility appropriateness of modeling languages. In: MoDELS, Springer, pp 691–705
41. Hadar E, Hassanzadeh A (2019) Big data analytics on cyber attack graphs for prioritizing agile security requirements. In: 2019 IEEE 27th International Requirements Engineering Conference (RE), IEEE, pp 330–339
42. Hele-Mai H, Tanel-Lauri L (2001) A survey of concept-based information retrieval tools on the web. In: Proceedings of the 5thEast-European Conference AD BIS, pp 29–41
43. Herre H (2010) General formal ontology (gfo): A foundational ontology for conceptual modelling. In: Theory and applications of ontology: computer applications, Springer, pp 297–345
44. Iannacone M, Bohn S, Nakamura G, Gerth J, Huffer K, Bridges R, Ferragut E, Goodall J (2015) Developing an ontology for cyber security knowledge graphs. In: Proceedings of the 10th Annual Cyber and Information Security Research Conference, ACM, New York, NY, USA, CISR '15, pp 12:1–12:4
45. Islam C, Babar MA, Nepal S (2019) Automated Interpretation and Integration of Security Tools Using Semantic Knowledge. Springer International Publishing, DOI 10.1007/978-3-030-21290-2_32
46. ISO Central Secretary (2011) Information technology — Security techniques — Information security risk management. Standard ISO/IEC 27005:2011, International Organization for Standardization, Geneva
47. ISO Central Secretary (2012) Information technology — security techniques — guidelines for cybersecurity. Standard ISO/IEC 27032:2012, International Organization for Standardization, Geneva

48. ISO Central Secretary (2018) Information technology — security techniques — information security management systems — overview and vocabulary. Standard ISO/IEC 27000:2018-02, International Organization for Standardization, Geneva
49. ISO Central Secretary (2018) Information technology — Security techniques — Information security risk management. Standard ISO/IEC 27005:2018, International Organization for Standardization, Geneva
50. Jacobsen A, de Miranda Azevedo R, Juty NS, Batista D, Coles SJ, Cornet R, Courtot M, Crosas M, Dumontier M, Evelo CTA, Goble CA, Guizzardi G, Hansen KK, Hasnain A, Hettne KM, Heringa J, Hooft RWW, Imming M, Jeffery KG, Kaliyaperumal R, Kersloot MG, Kirkpatrick CR, Kuhn T, Labastida I, Magagna B, McQuilton P, Meyers N, Montesanti A, van Reisen M, Rocca-Serra P, Pergl R, Sansone S, da Silva Santos LOB, Schneider J, Strawn GO, Thompson M, Waagmeester A, Weigel T, Wilkinson MD, Willighagen EL, Wittenburg P, Roos M, Mons B, Schultes E (2020) FAIR principles: Interpretations and implementation considerations. Data Intell 2(1-2):10–29, DOI 10.1162/dint_r_00024
51. Jia Y, Qi Y, Shang H, Jiang R, Li A (2018) A practical approach to constructing a knowledge graph for cybersecurity. Engineering 4(1):53–60
52. Jurisica I, Mylopoulos J, Yu E (1999) Using ontologies for knowledge management: An information systems perspective. In: Proceedings of the Annual Meeting-American Society For Information Science, Information Today; 1998, vol 36, pp 482–496
53. Kang D, Lee J, Choi S, Kim K (2010) An ontology-based enterprise architecture. Expert Systems with Applications 37(2):1456–1464, DOI https://doi.org/10.1016/j.eswa.2009.06.073
54. Keil JM, Schindler S (2019) Comparison and evaluation of ontologies for units of measurement. Semantic Web 10(1):33–51
55. Kiesling E, Ekelhart A, Kurniawan K, Ekaputra F (2019) The SEPSES Knowledge Graph: An Integrated Resource for Cybersecurity, vol 11779 LNCS. Springer International Publishing, DOI 10.1007/978-3-030-30796-7_13
56. Langer L, Smith P, Hutle M (2015) Smart grid cybersecurity risk assessment. In: 2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST), pp 475–482, DOI 10.1109/SEDST.2015.7315255
57. Lassila O, McGuinness D (2001) The role of frame-based representation on the semantic web. Linköping electronic articles in computer and information science 6(5):2001
58. Li K, Zhou H, Tu Z, Feng B (2020) CSKB: A Cyber Security Knowledge Base Based on Knowledge Graph, vol 1268 CCIS. Springer Singapore, DOI 10.1007/978-981-15-9129-7_8
59. Martins BF, Serrano L, Reyes JF, Panach JI, Pastor O, Rochwerger B (2020) Conceptual characterization of cybersecurity ontologies. In: 13th IFIP WG 8.1 working conference on the Practice of Enterprise Modelling (PoEM 2020), Springer, pp 323–338
60. Martins BF, Serrano L, Reyes JF, Panach JI, Pastor O (2021) Towards the Consolidation of Cybersecurity Standardized Definitions. Tech. Rep. Version 2,

Universidad Politecnica de Valencia, URL http://hdl.handle.net/10251/163895
61. Martins BF, Serrano L, Reyes JF, Panach JI, Pastor O (2021) Towards the consolidation of cybersecurity standardized definitions: a tool for ontological analysis. In: Proceedings of the XXIV Iberoamerican Conference on Software Engineering, CIbSE 2021, San José, Costa Rica, 2021, pp 1–14
62. Mascardi V, Cordì V, Rosso P (2007) A comparison of upper ontologies. In: Woa, vol 2007, pp 55–64
63. Masolo C, Borgo S, Gangemi A, Guarino N, Oltramari A, Schneider L (2002) The wonderweb library of foundational ontologies: preliminary report. WonderWeb Deliverable D 17
64. Masolo C, Borgo S, Gangemi A, Guarino N, Oltramari A (2003) Wonderweb deliverable d18 ontology library (final). ICT project 33052:31
65. Mizoguchi R, Ikeda M (1998) Towards ontology engineering. Journal-Japanese Society for Artificial Intelligence 13:9–10
66. Möller DPF (2020) Cybersecurity Ontology, Springer Cham, pp 99–109. DOI 10.1007/978-3-030-60570-4_7
67. Mozzaquatro BA, Agostinho C, Goncalves D, Martins J, Jardim-Goncalves R (2018) An ontology-based cybersecurity framework for the internet of things. Sensors 18(9):3053
68. Mundie DA, Ruefle R, Dorofee AJ, Perl SJ, McCloud J, Collins M (2014) An incident management ontology. In: STIDS, pp 62–71
69. Narayanan S, Ganesan A, Joshi K, Oates T, Joshi A, Finin T (2018) Cognitive techniques for early detection of cybersecurity events. arXiv preprint arXiv:180800116
70. Nurse JRC, Creese S, Goldsmith M, Lamberts K (2011) Trustworthy and effective communication of cybersecurity risks: A review. In: 2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST), pp 60–68, DOI 10.1109/STAST.2011.6059257
71. Obrst L, Chase P, Markeloff R (2012) Developing an ontology of the cyber security domain. In: STIDS, pp 49–56
72. Oltramari A, Kott A (2018) Towards a reconceptualisation of cyber risk: An empirical and ontological study. Journal of Information Warfare 17(1):49–73
73. Oltramari A, Vetere G, Lenzerini M, Gangemi A, Guarino N (2010) Senso comune. In: LREC
74. Oltramari A, Cranor LF, Walls RJ, McDaniel PD (2014) Building an ontology of cyber security. In: STIDS, Citeseer, pp 54–61
75. Oltramari A, Cranor LF, Walls RJ, McDaniel P (2015) Computational ontology of network operations. In: MILCOM 2015-2015 IEEE Military Communications Conference, IEEE, pp 318–323
76. Oltramari A, Henshel DS, Cains M, Hoffman B (2015) Towards a human factors ontology for cyber security. In: STIDS, pp 26–33
77. Onwubiko C (2018) Cocoa: An ontology for cybersecurity operations centre analysis process. In: 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp 1–8
78. Ou X, Govindavajhala S, Appel AW (2005) Mulval: A logic-based network security analyzer. In: USENIX security symposium, Baltimore, vol 8, pp 113–

128
79. Parmelee MC (2010) Toward an ontology architecture for cyber-security standards. STIDS 713:116–123
80. Peciña K, Bilbao A, Bilbao E (2011) Physical and logical security risk analysis model. In: 2011 Carnahan Conference on Security Technology, pp 1–7, DOI 10.1109/CCST.2011.6095895
81. Pipa AMC (2018) Owl ontology quality assessment and optimization in the cybersecurity domain. PhD thesis, Instituto Universitário de Lisboa
82. Qin S, Chow KP (2019) Automatic Analysis and Reasoning Based on Vulnerability Knowledge Graph. In: Ning H (ed) Communications in Computer and Information Science, vol 1137 CCIS, Springer Singapore, Singapore, pp 3–19, DOI 10.1007/978-981-15-1922-2_1
83. Sales TP, Guizzardi G (2019) Ontological anti-patterns in taxonomic structures. In: ONTOBRAS
84. Sales TP, Baião F, Guizzardi G, Almeida JPA, Guarino N, Mylopoulos J (2018) The common ontology of value and risk. In: International Conference on Conceptual Modeling, Springer, pp 121–135
85. Scarpato N, Cilia ND, Romano M (2019) Reachability matrix ontology: a cybersecurity ontology. Applied Artificial Intelligence 33(7):643–655
86. Schumacher M (2003) 6. toward a security core ontology. In: Security engineering with patterns, Springer, pp 87–96
87. Serrano L, Martins BF, Serrano JF, Panach JI, Pastor O (2021) Una encuesta acerca de la Definición de Conceptos de Ciberseguridad. Tech. Rep. Version 1, Universidad Politecnica de Valencia, URL https://riunet.upv.es/handle/10251/174756
88. Sikos LF (2019) OWL Ontologies in Cybersecurity: Conceptual Modeling of Cyber-Knowledge, Springer International Publishing, Cham, pp 1–17
89. Simperl E, Bürger T, Hangl S, Wörgl S, Popov I (2012) Ontocom: A reliable cost estimation method for ontology development projects. Journal of Web Semantics 16:1–16
90. Singhal A, Ou X (2017) Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs, Springer International Publishing, pp 53–73
91. Souag A, Salinesi C, Comyn-Wattiau I (2012) Ontologies for security requirements: A literature survey and classification. In: International conference on advanced information systems engineering, Springer, pp 61–69
92. Studer R, Benjamins VR, Fensel D (1998) Knowledge engineering: principles and methods. Data & knowledge engineering 25(1-2):161–197
93. Syed R (2020) Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. DOI 10.1016/j.im.2020.103334
94. Syed R, Zhong H (2018) Cybersecurity vulnerability management: An ontology-based conceptual model
95. Syed Z, Padia A, Finin T, Mathews L, Joshi A (2016) UCO: A unified cybersecurity ontology. In: Workshops at the Thirtieth AAAI Conference on Artificial Intelligence
96. Takahashi T, Kadobayashi Y (2011) cybersecurity information exchange techniques: Cybersecurity information ontology and cybex. Journal of the National

Institute of Information and Communications Technology Vol 58(3/4)
97. Takahashi T, Kadobayashi Y (2015) Reference ontology for cybersecurity operational information. The Computer Journal 58(10):2297–2312
98. Takahashi T, Fujiwara H, Kadobayashi Y (2010) Building ontology of cybersecurity operational information. In: Proceedings of the Sixth Annual Workshop on Cyber Security and Information intelligence Research, pp 1–4
99. Takahashi T, Kadobayashi Y, Fujiwara H (2010) Ontological approach toward cybersecurity in cloud computing. In: Proceedings of the 3rd international conference on Security of information and networks, pp 100–109
100. Tissir N, El Kafhali S, Aboutabit N (2020) Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. Journal of Reliable Intelligent Environments DOI 10.1007/s40860-020-00115-0, URL https://doi.org/10.1007/s40860-020-00115-0
101. Undercofer J, Joshi A, Finin T, Pinkston J, et al. (2003) A target-centric ontology for intrusion detection. In: Workshop on Ontologies in Distributed Systems, held at The 18th International Joint Conference on Artificial Intelligence
102. Uschold M, Gruninger M (2004) Ontologies and semantics for seamless connectivity. ACM SIGMod Record 33(4):58–64
103. Uschold M, Gruninger M, et al. (1996) Ontologies: Principles, methods and applications. TECHNICAL REPORT-UNIVERSITY OF EDINBURGH ARTIFICIAL INTELLIGENCE APPLICATIONS INSTITUTE AIAI TR
104. Van Heijst G, Schreiber AT, Wielinga BJ (1997) Using explicit ontologies in kbs development. International journal of human-computer studies pp 183–292
105. Wand Y, Weber R (1995) On the deep structure of information systems. Information Systems Journal 5(3):203–223
106. Wang JA, Guo M (2009) Ovm: an ontology for vulnerability management. In: 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, pp 1–4
107. Wang JZ, Ali F (2005) An efficient ontology comparison tool for semantic web applications. In: The 2005 IEEE/WIC/ACM International Conference on Web Intelligence (WI'05), IEEE, pp 372–378
108. Wieringa R (2014) Design Science Methodology for Information Systems and Software Engineering. Springer
109. Zuanelli E (2017) The cybersecurity ontology platform: the poc solution. e-AGE2017 p 1