Conceptual Characterization of Cybersecurity Ontologies

Beatriz F. Martins, Lenin Serrano, José F. Reyes, José Ignacio Panach, Oscar Pastor, Benny Rochwerger

▶ **To cite this version:**

Beatriz F. Martins, Lenin Serrano, José F. Reyes, José Ignacio Panach, Oscar Pastor, et al.. Conceptual Characterization of Cybersecurity Ontologies. 13th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling (PoEM 2020), Nov 2020, Riga, Latvia. pp.323-338, 10.1007/978-3-030-63479-7_22 . hal-03434647

HAL Id: hal-03434647
https://inria.hal.science/hal-03434647

Submitted on 18 Nov 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Conceptual Characterization of Cybersecurity Ontologies*

Beatriz F. Martins[1][0000−0001−9190−1047], Lenin Serrano[1,2][0000−0002−1631−7139], José F. Reyes[1][0000−0002−9598−1301], José Ignacio Panach[3][0000−0002−7043−6227], Oscar Pastor[1][0000−0002−1320−8471], and Benny Rochwerger[4]

[1] PROS Research Center, Universitat Politècnica de València, Camino de Vera s/n, 46022 Valencia, Spain, {bmartins, lserrano, jreyes@}@pros.upv.es,opastor@dsic.upv.es
[2] Ingeniería de Sistemas e Informática, Universidad Pontificia Bolivariana Km 7 via Bucaramanga - Piedecuesta, Santander, Colombia
[3] Escola Tècnica Superior d'Enginyeria, Universitat de València, Avinguda de l'Universitat, 46100 Burjassot, Valencia joigpana@uv.es,
[4] Accenture Israel Cyber R&D Lab, Tel Aviv, Israel benny.rochwerger@accenture.com

Abstract. Cybersecurity is known as the practice of protecting systems from digital attacks. Organizations are seeking efficient solutions for the management and protection of their assets. It is a complex issue, especially for great enterprises, because it requires an interdisciplinary approach. The kinds of problems enterprises must deal with and this domain complexity induces misinterpretations and misunderstandings about the concepts and relations in question. This article focus on dealing with Cybersecurity from an ontological perspective. The first contribution is a search of previously existing works that have defined Cybersecurity Ontologies. The paper describes the process to search these works. The second contribution of the paper is the definition of characteristics to classify the papers of Cybersecurity Ontologies previously found. This classification aims to compare the previous works with the same criteria. The third contribution of the paper is the analysis of the results of the comparison of previous works in the field of Cybersecurity Ontologies. Moreover, the paper discusses the gaps found and proposes good practice actions in Ontology Engineering for this domain. The article ends with some next steps proposed in the evolution towards a pragmatic and iterative solution that meets the needs of organizations.

Keywords: Cybersecurity · Ontology · Knowledge Graphs · Organizations · Enterprise Architecture

* This work has been developed under the project Digital Knowledge Graph – Adaptable Analytics API with the financial support of Accenture LTD. Also, *In Memorian* of Prof. Ricardo Almeida Falbo from NEMO-UFES, Brazil.

1 Introduction

Organizations are actively seeking efficient solutions for the management and protection of their digital assets. The Cybersecurity domain contributes to the basic protection of *confidentiality*, *integrity*, and *availability* of information from ISO/IEC 27032 [5] since it relates to actions that rely on information security, application security, and network security. However, Cybersecurity is a domain constantly evolving, always adopting new technologies bringing great concerns to organizations; especially in terms of Enterprise Architecture. Besides, not only technological aspects are relevant, because the weakest link in the chain to guarantee information security is the human factor. This ranges from the behavior of users and attackers to the way in which each stakeholder within the organization participates and understands the concepts and relationships in which they are inserted.

The kinds of problems enterprises must deal with and this domain complexity induce misinterpretations and misunderstandings about the concepts and relations in question. Indeed these problems arise when it is necessary to ensure effective communication among humans, among systems or between humans and systems [27]. Moreover, each person is dealing with the information according to their own perception depending on the role each stakeholder plays in the enterprise and this interferes with the strategies adopted w.r.t. the Enterprise Architecture. For instance, the term "Risk" may be controversial. While a manager can think about this concept in a general perception ("*How much does it cost and what is the benefit?*"), a security engineer can think about the same term but with a specific perception ("*What data we may lose and what is the impact?*"). Both roles think they are talking about the same concept but, in fact, this is not the truth. 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 [6], while the latter is talking about a standard perspective like the ISO/IEC 27000 [7]. In this case, both are definitions for the term "Risk" based on standards widely accepted by the cybersecurity community but they mean different "*things*" w.r.t its semantics.

The solutions adopted are interdisciplinary. On one hand, the security requirement community addresses this challenge by using graph approaches that provide practical mechanisms of analysis [45]. This approach is known as Attack Graph (AG) [22] which is a kind of Knowledge Graph(KG) [25]. These are methods to explore the security among assets and possible attacks (i.e., risks). In addiction, the Industry 4.0 recently adopted the use of Digital Twins Graphs [9] that provide statistical methods, data analytics by using machine learning techniques over a simulation environment. On the other hand, conceptual modeling, more specifically the branch of ontologies in computer and information sciences,

[5] https://www.iso.org/standard/44375.html
[6] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
[7] https://www.iso.org/standard/73906.html

has been a tool used to deal with elements constituting a conceptualization of a given domain [16]. This approach allows articulating abstractions of a certain state of affairs in reality. Cybersecurity KGs are implementations of conceptualizations that intent to provide data analysis. In this sense, ontologies are a natural choice on providing grounding for KGs.

The grounding of concepts is one of the most important ontology applications [16] and a KG may be considered an implementation of a conceptualization (an Operational Ontology) [20]. Thus, the conceptual modeling through an ontological approach is fundamental to make explicit concepts and to facilitate human comprehension about them [14]. However, there is no definitive architectural solution for the design and development of KGs supported by ontologies yet.

Since this issue is complex and interdisciplinary, the first contribution of this paper is an initial study of existing works that deal with cybersecurity requirements from an ontological perspective. For each existing work, we:

- identify proposals in the cross-field of Cybersecurity and Ontologies;
- evaluate the existing Cybersecurity Ontologies' level of applicability;
- identify the possible data sources of cybersecurity information.

The second contribution of this paper is to classify the results from the previous study of the existing works into characteristics. For this aim, we define a set of criteria for comparing the ontologies found in the previous works review. This classification helps compare ontologies among them with the same criteria. Finally, the third contribution is the proposal of solutions to improve the ontology definition in the Cybersecurity domain. These solutions aim to solve most of the problems detected during the analysis of the previous existing works.

We have organized the rest of this paper as follows: Section 2 presents other works who performed the comparison of ontologies. Section 3 presents how we looked into the literature for previous works in the field of cybersecurity ontologies. Section 4 proposes a classification of the previous works. Section 5 presents the analysis of the found works. Section 6 discusses the results and propose some solution to solve found problems in the previous works. Section 7 draws conclusions and discusses some further research directions.

2 Related Works

There are a few literature review papers in the context of Cybersecurity Ontologies. This is because studies on this topic are recent, as well as their applications in Cybesecurity. The first ontologies we found in our literature review were published together with the first works focused on Ontology-Driven Conceptual Modeling. However, the practical use of these ontologies has only recently started. In our analysis we did not find any systematic literature review covering this specific domain and the reviews we found appear as sample papers.

The work of Leslie Sikos [44] presents a literature review in the context of Cybersecurity Ontologies. This related work introduces multiple classifications

but the orthogonality relationship among those is not clear, sometimes mixing. Besides, the authors focus only on triple-stores (Resource Description Framework (RDF) [8] triples) setting aside Not Only SQL (NoSQL) platforms. The gray work [41] goes in the same direction but focusing on the Ontology Web Language (OWL) [9] approach. By contrast, we make no distinction as to the language or implementation used because it is important for us to know any practical approach to bring the state-of-the-art closer to the state-of-practice.

Aside from the Cybersecurity domain, there are several works comparing other domain ontologies; however most of them focus the comparison criteria on conceptual matching. Their objective is to verify if a concept present in different ontologies has the same meaning by verifying formal characteristics (at the ABox [10]). The work of Keil [28] presents a summary of those approaches. At the same direction there are even proposals for tools to automate this task [54]. The systematic literature review [5] covers the ontologies at the Security domain. Their comparison criteria also focus on implementation in OWL, RDF, and DARPA Agent Markup Language (DAML) [11]. These approaches go in the opposite direction from ours, since our focus is on conceptualization itself (at the TBox [12]). The work of Mascardi [29] compares foundational ontologies. Although it is interesting from the ontological perspective we consider, it is dealing with a higher level of abstraction. Thus, it is a job to consider within the Ontology Engineering process, not in our current research.

As conclusion of the related works, we highlight that the few works that focus on comparing Cybersecurity Ontologies do not classify the results into characteristics and the sample used for the analysis is reduced.

3 Looking for Cybersecurity Ontologies in the Literature

In our research we apply the Design Science Methodology [56] with the final target to provide a tool able to create, manage, and integrate KGs supported by a well-designed ontology. We are dealing with the domain of Cybersecurity both in the context of Ontology and Software Engineering to produce an efficient KG management tool. The first step is to know what are the state-of-art of ontologies covering the cybersecurity domain, if they provide KG implementations, and what are their technical approaches. The research questions in the Design Science of this first step 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 for Cybersecurity Ontologies and what are their technical approach?

[8] http://www.w3.org/TR/rdf-mt/
[9] https://www.w3.org/TR/owl2-syntax/
[10] ABox statements represent instances of associated concepts at the knowledge base.
[11] http://www.daml.org/
[12] TBox statements describe the domain by defining its concepts and relations.

We start from a selection of a sample search chain [13]. However, we considered this is a handful amount, thus in further work, we plan to perform detailed analysis with diverse and more extended search chains. Our selection's criteria is applied in three steps. In the first step we focus on searching into the publication title. In the second step we read the abstract, and finally in the third step we read the whole document. In each step, we reject papers not accessible for reading, papers with low relevance by number of its citations, or papers that do not present effectively any proposal of ontology. Looking for the term in the title of publications at the most relevant sources, we found 198 papers, being: none at ACM, 1 at Springer, none at IEEE, none at Scopus, and 197 at Google Academic. In the second step of our filtering, after removing the papers in which the abstract was out of the target, we reduced the sample to 32. From those, during the reading process, we rejected 3 for lack of access to reading and 4 for not presenting ontologies. Finally, we reduced our sample to 25 publications, with a total of 19 ontologies because 6 papers refer to the same ontology (duplicated or complementary). This work of searching was carried out by two researchers (a *Domain Specialist* and an *Ontology Engineer*).

4 Characteristics to Compare Cybersecurity Ontologies

We define the set of characteristics to allow an orthogonal comparison of the works found. We consider two viewpoints: the ontological perspective as a conceptual modeling approach and the domain of knowledge on cybersecurity perspective. The former looks for the aspect of the semantic foundation, while the latter deals with the knowledge domain itself. The proposal of this classification is based on previous works related with the types of ontologies. Note that one of the contributions of this work is to assemble all the classifications specifically for the context of cybersecurity ontologies.

4.1 Ontological Perspective

Next we describe the characteristics to classify the previous works according to the ontological perspective:

Level of Applicability: It is necessary to take into account the difference between *Operational Ontologies* and *Reference Ontologies* [20]. A Reference Ontology should be a conceptualization constructed to make the best possible description of the domain concerning a certain level of granularity and point of view. An Operational Ontology is the actionable version of a Reference Ontology that uses the more appropriate language intending to guarantee desirable computational properties without compromising the previously defined ontological commitment [17]. Therefore, there should be no operational ontology without the existence of data and their relationships as instances of previously well-defined

[13] Search chain, accessed on April 2020: ($TITLE$ = "*Cybersecurity Ontology*") or ("*Cybersecurity Ontologies*") when it is not possible filter by title.

concepts. In this sense, the classification of ontologies according to its level of applicability (Reference or Operational) is our base analysis criteria.

Reference Ontology supporting the implementation: The existence or not of a Reference Ontology before its implementation depends on the choice of the design methodology used. Several methodologies drive the ontologies design process, however, there is no consensus about this matter. The methodology SaBio [11] requires that the Reference Ontology precedes its Operational Ontology but the most known and used methodology, the *Methontology* [12], does not. There is also a methodological approach domain-specific [33] that strives the cybersecurity ontology design according to a three-layer architecture –Upper, Mid-level and Domain Ontologies. Thus, we also consider the adopted design methodology as an aspect related to analysis of the level of applicability.

Level of Generality: This characteristic classifies the ontologies according to Guarino's proposal [16]. In this case, ontologies are classified according to its level of generality in four types: *Foundational Ontologies* (also known as *High-level Ontologies*), *Domain Ontologies*, *Task Ontologies*, or *Application Ontologies*.

Ontology Grounding though a Foundational Ontology: For the generality level classification, it is important to identify if the cybersecurity ontologies are well-grounded through some Foundational Ontology. In this case, we are looking for groundings like BWW [53], GFO/GOL [8,23], DOLCE [7], UFO [19,21], or other Foundational Ontology. Only then, we determine the generality level of the paper presented cybersecurity ontology itself, identifying if they are Domain, Task, or Application Ontologies. Eventually, if these ontologies may be classifiable as *Core Ontologies* [14].

4.2 Cybersecurity Perspective

The ISO/IEC 27032 and ISO/IEC 27000 standards compose the knowledge base to identify and find out definitions to the most used terms in the development of ontologies in the domain of cybersecurity. One of the contributions of this paper is using all these standards as characteristics to classify the found works of cybersecurity ontologies. Next, we describe these characteristics.

ISO/IEC 27032: The term cybersecurity is defined in the ISO/IEC 27032 standard as a response to technological development and communications today. The ISO/IEC 27032 promotes procedures to establish and maintain security in cyberspace in the dimensions of *Confidentiality*, *Availability*, and *Integrity*. The ISO/IEC 27032 offers technical guidance focused on closing the gap between different security domains. We use for our terminological verification the chapter 4 (numeral from 1 to 58) and from chapters 8 and 9.

ISO/IEC 27000: The ISO/IEC 27000 provides an overview of *Information Security Management Systems* and documents the general terminology used in the cybersecurity domain. Together with the ISO/IEC 27032, the ISO/IEC 27000

[14] The Core Ontologies classifies ontologies between the Foundational and Domain Ontologies, not so general as the firsts either so specific as the latter's.

proposes controls for risk management, attack identification, detection, monitoring, and incident response. Therefore, these are standards designed to guide the treatment of cybersecurity risks. We consider on our terminological verification the ISO/IEC 27000 definitions documented in chapter 3 (numeral 1 to 77).

Terminological Verification: The last classification we consider is the ISO/IEC 27032 and the ISO/IEC 27000 terminological verification (those terms whose definition is provided at these standards) applied to the papers we found. We aim to know which are the most used terms (concepts) in the papers to compare which notions of cybersecurity each of the selected ontologies uses (for example, if they all have the concept of vulnerability, threat, etc.). Thus, we used a semi-automatic technique to run a regular expression search algorithm [42] we developed to extract each of the exact ISO/IEC terms. After the automatic extraction we perform a second round of papers' reading to verify if all terms comply with their cybersecurity ontology's context. We found a total of 156 terms from the ISO/IEC definitions complying with ontological concepts, and we count the number of its citations.

5 Cybersecurity Ontologies Analysis

This section analyzes the works found in the literature. We present these works grouping them by their most relevant characteristic, w.r.t the established ontological perspective.

5.1 Reference Ontologies

The Vulnerability Description Ontology (VDO) [6] proposal presents a conceptualization by means of natural language descriptions. Thus, the VDO describes the most relevant concepts for vulnerability management. The VDO framework provides a proper syntax to describe characteristics, valid values, and relationships about the domain (a Domain Ontology). Those are terms supported by cybersecurity Common Vulnerabilities and Exposures (CVE) [15] knowledge base from MITRE corporation.

The Conceptual Model of Vulnerability Ontology [46] is an ontology-based conceptual model for ontological representation of the cybersecurity vulnerability domain (a Domain Ontology) that is a specific part under the cybersecurity universe. Thus, this ontology complies with information security standards and incorporates social media concepts.

The Ontology-based cyber security model (Malware Ontology) [15] presents a conceptualization of the malware behavior. The authors present their approach as a work in progress since they plan developments on reasoning and detection procedures. The Malware Ontology is an ontology written with OWL but not implemented yet. It is not grounded over any Foundational Ontology.

[15] https://cve.mitre.org/

5.2 Operational Ontologies

The Intrusion Detection System ontology (IDS) [52] is a Target-Centric Ontology for Intrusion Detection implemented with DAML+OIL[24] and provide reasoning. As it is a Core Ontology being one of the first initiatives on cybersecurity ontologies, but there are no foundational grounding notions in terms of semantics. This happens because Description Logics (DL) [1] grounds DAML+OIL and it is neutral in terms of ontological level [17].

The Unified Cybersecurity Ontology (UCO) [47] is an extension of the IDS ontology for integration and cyber situational awareness. The UCO has an OWL implementation and intents to capture the cybersecurity domain of Knowledge committed with many cybersecurity standards. It also is considered a Domain Ontology since it has focused only on the cybersecurity conceptualization. However, there is no mention of any strong foundational grounding. In summary UCO is essentially an ontology under the Linked Data [4] perspective.

The Semantic Cyber Incident Classification (SCIC) [10] presents a set of steps to produce an Operational Ontology with OWL [16] employing a compilation of different data sources. The SICS focus on the cybersecurity insurance domain providing classification for cybersecurity incidents, so it is a Domain Ontology. However, the SCIC approach does not provide a mechanism to avoid misunderstandings when it is necessary to manipulate, update, or add new information from additional data sources (other than the initial ones). In other words, as SCIC constitutes a compendium of several approaches not supported by any Foundational Ontology, the resulting semantics from the implementation changes along with the data sources taken over time.

At the *Internet of Things* (IoT) context, the proposal of an Ontology-Based Cybersecurity Framework [30] provides the IoTSec ontology focusing on the enterprise viewpoint (a Domain Ontology). The framework has three layers, in which the IoTSec ontology appears as a *layer integrator* solution for semantic adequacy and reasoning. The IoTSec ontology[17] is an Operational Ontology implemented with OWL with reasoning capabilities. They provide a Java API for RESTful Web Services (JAX-RS) that addresses the enterprise modeling mechanisms (BPMN notation) to the knowledge base.

The Incident Management Ontology (IM) [31] starts from a metamodel intent to capture a variety of incident management process models. It is an Operational Ontology implemented in OWL with Protègè[18] and according to the Methontology approach. Although the IM ontology is supported by cybersecurity standards for incident management (Domain Ontology), the project was done in an inverse way to the usual, where ontologies support the metamodels for Domain-Specific Languages (DSL) and not the reverse.

The framework MulVAL [39] –Multihost, Multistage, Vulnerability Analysis– uses the Datalog language as the implementation that is a subset of Prolog. This

[16] https://www.w3.org/TR/owl2-syntax/
[17] https://github.com/brunomozza/IoTSecurityOntology/blob/master/iotsec.owl
[18] https://protege.stanford.edu/

framework aims to model the software bugs' interaction with the system and network configurations and provides a reasoning engine for such. The framework MulVAL can be considered 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) [19] that 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.

The Cyber Ontology [40,33] is an implementation developed by the MITRE Co [20]. It has a large number of the RDF instances and incorporates a sort of ontologies: the Dublin Core metadata standard ontology [21], parts of the Simple Knowledge Organization System (SKOS) [22], a Point-of-Contact ontology [23] (grounded over FOAF [24] and VCard ontologies), and Content Curation ontology.

A knowledge-base focusing at the cybersecurity domain divided into three sub-ontologies –Assets (OS and Software), Vulnerability, and Attack(DDos and Control Class) [26] presents an approach based on machine learning principles to provide an Operational Ontology. The proposal aggregates concepts obtained from cybersecurity sources (or ontologies) by means of the Stanford NER [13] to provide many different KG instances for each of those sub-ontologies. Although operational, it is not grounded over any foundational ontology. On the contrary, the ontology here is closer to the result than a support for the process.

The Cognitive CyberSecurity (CCS) [32] approach implements KGs from an extension of the UCO for event detection context. This proposal is an Operational Ontology implemented with OWL and the Semantic Web Rule Language (SWRL)[25] for entity relational rules that provide CCS based on KGs. The CCS can be considered an Application Ontology since it deals with tasks for event detection at the cybersecurity domain.

The Ontology of Cybersecurity of Critical Infrastructures [3] is implementation made with OWL and using the TopBraid ME Composer [26]. Four sub-ontologies compounds this ontology: IT-Security, Project, Critical Infrastructure (CRITIS), and Compliance. Although it is a conceptualization supported by a set of cybersecurity standards (Domain Ontology), there are no Foundational Ontology grounding those concepts.

The *"Piattaforma Ontologica della Cybsersecurity"* (POC) [57] is a pragmatic approach for representing the cybersecurity knowledge. It is also a three-layer ontology [33] and can be a conceptualization classified as an Application Ontology because additionally to the domain aspects deals with activities of this domain pragmatically. This ontology is also in the Linked Data context.

[19] http://oval.mitre.org/documents/docs-03/intro/intro.html
[20] http://cve.mitre.org
[21] http://dublincore.org/documents/dces/
[22] http://www.w3.org/2004/02/skos/
[23] http://www.w3.org/Submission/vcard-rdf/
[24] http://xmlns.com/foaf/spec/
[25] https://www.w3.org/Submission/SWRL/
[26] https://www.topquadrant.com/

5.3 Operational Ontologies with previous Reference Ontology

The Cybersecurity Operations Center Ontology for Analysis (CoCoa) [38] aims to help in the understanding of how cyber incidents may be detected in a monitored environment. Although the authors define CoCoa as a process ontology, it is an Application Ontology for the Cybersecurity domain that deals with incidents monitoring through logs and network information, having data tasks like source, sense, detect, respond and recover. The Reference Ontology produces its operational version implemented through a KG able to provide analytics.

The Ontology for Vulnerability Management (OVM) [55] is an ontology implemented through DL grounding (DL is ontologically neutral). Although this conceptualization is supported by well-known cybersecurity standards, it is not grounded over any Foundational Ontology.

The Ontology of Cybersecurity Operational Information [49,48] proposes a conceptualization covering three main domains: The Incident Handling Domain, IT Asset Management Domain, and Knowledge Accumulation Domain. Those domains compose sub-ontologies under the Operational Information perspective (Domain Ontology), where the proposal discusses entities and relations related to (Reference Ontology). The approach [51] extends the ontology to the context of cloud computing and proposes an implementation for that. This proposal [50] is integrated with CYBEX [43].

5.4 Well-grounded Ontology

The CRATELO [35,36] is a three-layer ontology [33] proposal for the domain of cybersecurity (Domain Ontology). It is grounded over a Foundational Ontology named DOLCE-SPRAY [37], 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-DL and SWRL with Protègè. The CRATELO has some extensions described in [34,2].

5.5 Comparative Frame

Table 1 presents a summary of the ontology characterization we made according to the orthogonal criteria we propose. From 25 papers (19 ontologies) we found: 5 are only Reference Ontologies and 20 Operational Ontologies, 4 of those are supported by a Reference Ontology. Some works refer to the same ontology, therefore, we found a total of 19 ontologies in this research work.

6 Discussion

In this scenario the most significant information we extract is the lack of foundational grounding in the cybersecurity ontologies we found. Only, four papers mention a foundational grounding and all of them are related to the

Table 1. Summary of Cybersecurity Ontologies Characterization.

	Level of Applicability		Level of Generality	
Proposed Ontology	**Reference Ontology**	**Operational Ontology**	**Foundational Ontology**	**Guarino's [17] Classification**
CCS [32]	No	Yes	No	Domain Ontology
CoCoa [38]	Yes	Yes	No	Application Ontology
Conceptual Model of Vulnerability Ontology [46]	Yes	No	No	Domain Ontology
CRATELO [35]	No	Yes	Yes	Application Ontology
CRATELO [36]	No	Yes	Yes	Domain Ontology
CRATELO [34]	No	Yes	Yes	Domain Ontology
CRATELO [2]	No	Yes	Yes	Domain Ontology
Cyber Ontology [40]	No	Yes	No	Application Ontology
IDS [52]	No	Yes	No	Core Ontolgy
IM [31]	No	Yes	No	Domain Ontology
IoTSec [30]	No	Yes	No	Domain Ontology
Knowledge-Base focusing at the cybersecurity domain [26]	No	Yes	No	Domain Ontology
Malware Ontology [15]	Yes	No	No	Domain Ontology
MITRE Co approach [33]	No	Yes	No	Core Ontolgy
MulVAL [39]	No	Yes	No	Application Ontology
Ontology of Cybersecurity of Critical Infrastructures [3]	No	Yes	No	Domain Ontology
Ontology of Cybersecurity Operational Information [50]	Yes	Yes	No	Domain Ontology
Ontology of Cybersecurity Operational Information [49]	Yes	No	No	Domain Ontology
Ontology of Cybersecurity Operational Information [51]	Yes	Yes	No	Domain Ontology
Ontology of Cybersecurity Operational Information [48]	Yes	No	No	Domain Ontology
OVM [55]	Yes	Yes	No	Domain Ontology
POC [57]	No	Yes	No	Application Ontology
SCIC [10]	No	Yes	No	Domain Ontology
UCO [47]	No	Yes	No	Domain Ontology
VDO [6]	Yes	No	No	Domain Ontology

CRATELO [35,36,34,2] proposal. The importance of a conceptual basis is clear when the support of a Foundational Ontology avoids semantic interoperability problems on Domain Ontologies [18].

Besides the lack of grounding that we detect, most papers mentioning Operational Ontologies have been implemented without 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. Indeed, only the Ontology of Cybersecurity Operational Information [49,51,48,50], CoCoa [38], and OVM [55] proposals provide an Operational Ontology 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 [20].

The main cause of these problems results is from the ontology design methodologies adopted. In other words, they do not perceive that the best practices established in the Software Engineering Process can be knowledge already acquired used as part of the Ontology Engineering Process. The SaBio [11] methodology is the only one we know that has a proposal to fulfill those gaps. Based on that, we suggest that Ontology Engineers must take some best-practice actions like:

- maintain efficient and high quality communication with Domain Experts stakeholders;
- take in use a methodology that drives the process by using Reference Ontologies before the implementation of Operational Ontologies;
- take in use a well-defined ontological grounding for the design process Reference Ontologies;

– adequately justify the reasons for not implementing a Reference Ontology (or because it is a project requirement itself or the reasons why the implementation was not viable). This is a methodological question still uncovered.

Table 2 presents most cited terms from the result of our regular expression search algorithm described in Section 4.2 through the cybersecurity perspective. We highlight main dimensions of security(*Availability*, *Confidentiality* and *Integrity*) that are essential properties present on all elements that require security control.

Table 2. Cybersecurity perspective – total of citations according to ISO/IEC 27000 and ISO/IEC 27032 terminology.

Term	Total of citations
Asset	348
Attack	942
Availability	61
Confidentiality	37
Control	154

Term	Total of cations
Event	333
Integrity	45
Malware	218
Organization	271
Policy	117

Term	Total of cations
Process	401
Risk	259
Stakeholder	50
Threat	348
Vulnerability	775

Cross-interpreting the two perspectives allows us to determine which cybersecurity concepts are most relevant to the ontology community and how they are (or should be) interpreted. Definitions used by standards such as those in ISO/IEC exist to clarify the interpretation of these terms. However, the standards use natural (or technical) language that leaves room for more diverse interpretations by the community. In other words, 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. The Table 2 shows statistics that are essential as a starting point for doing this analysis.

7 Conclusions

In this work we have three contributions. The first one is a a pilot review in the cross-disciplinary context of Cybersecurity and Ontologies with three research questions. The second contribution is a definition of a set of characteristics to classify the ontologies found previously. The third contribution is a clear comparison of Cybersecuruty Ontologies based on an orthogonal characterization. Moreover, we highlight three important lacks in the Ontology Engineering process involved. We also suggest as a solution a set of best-practices for Cybersecurity Ontologies implementation and also useful for ontology design and development in general.

We would like to clarify that this research is a first step to conduct a systematic research in the future. We are aware that the search string is very limited, but it is enough to look for the particularities of ontologies, like those presented by Leslie Sikos [44]. Therefore, we know the necessity of new further steps on refining the used terminology. This research is also the basis for other work on

the definition and design of a definitive and well-grounded architecture for KGs creation, update and manipulation.

References

1. Baader, F., Calvanese, D., McGuinness, D., Patel-Schneider, P., Nardi, D., et al.: The description logic handbook: Theory, implementation and applications. Cambridge university press (2003)
2. Ben-Asher, N., Oltramari, A., Erbacher, R.F., Gonzalez, C.: Ontology-based adaptive systems of cyber defense. In: STIDS. pp. 34–41 (2015)
3. Bergner, S., Lechner, U.: Cybersecurity ontology for critical infrastructures. In: KEOD. pp. 80–85 (2017)
4. Bizer, C., Heath, T., Berners-Lee, T.: Linked data: The story so far. In: Semantic services, interoperability and web applications: emerging concepts, pp. 205–227. IGI Global (2011)
5. Blanco, C., Lasheras, J., Valencia-García, R., Fernández-Medina, E., Toval, A., Piattini, M.: A systematic review and comparison of security ontologies. In: 3th International Conference on Availability, Reliability and Security. pp. 813–820. IEEE (2008)
6. Booth, H., Turner, C.: Vulnerability description ontology (vdo). A Framework for Characterizing Vulnerabilities. NIST (2016)
7. Borgo, S., Masolo, C.: Ontological Foundations of DOLCE, pp. 279–295. Springer Netherlands, Dordrecht (2010)
8. Degen, W., Heller, B., Herre, H., Smith, B.: Gol: toward an axiomatized upper-level ontology. In: Proceedings of the international conference on Formal Ontology in Information Systems-Volume 2001. pp. 34–46 (2001)
9. Dietz, M., Putz, B., Pernul, G.: A distributed ledger approach to digital twin secure data sharing. In: IFIP Annual Conference on Data and Applications Security and Privacy. pp. 281–300. Springer (2019)
10. Elnagdy, S.A., Qiu, M., Gai, K.: 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). pp. 301–306. IEEE (2016)
11. Falbo, R.d.A.: SABiO: Systematic Approach for Building Ontologies. In: Proceedings of the 1st Joint Workshop ONTO.COM/ODISE on Ontologies in Conceptual Modeling and Information Systems Engineering (2014)
12. Fernández-López, M., Gómez-Pérez, A., Juristo, N.: Methontology: From ontological art towards ontological engineering. In: Proceedings of the Ontological Engineering AAAI-97 Spring Symposium Series. American Asociation for Artificial Intelligence (1997)
13. Finkel, J.R., Grenager, T., Manning, C.: Incorporating non-local information into information extraction systems by gibbs sampling. In: Proceedings of the 43rd Annual Meeting on Association for Computational Linguistics. p. 363–370. ACL '05, Association for Computational Linguistics, USA (2005)
14. Giaretta, P., Guarino, N.: Ontologies and knowledge bases towards a terminological clarification. Towards very large knowledge bases: knowledge building & knowledge sharing **25**, 32 (1995)
15. Grégio, A., Bonacin, R., Nabuco, O., Afonso, V.M., De Geus, P.L., Jino, M.: Ontology for malware behavior: A core model proposal. In: 2014 IEEE 23rd International WETICE Conference. pp. 453–458. IEEE (2014)

16. Guarino, N.: Formal Ontology in Information Systems. In: Proceedings of the 1st International Conference. pp. 6–8. IOS Press, Trento, Italy (June 1998)
17. Guarino, N.: The ontological level. Philosophy and the Cognitive Sciences (1994)
18. Guizzardi, G.: 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 (2006)
19. Guizzardi, G.: Ontological Foundations for Structural Conceptual Models. CTIT, Centre for Telematics and Information Technology (2005)
20. Guizzardi, G.: On ontology, ontologies, conceptualizations, modeling languages, and (meta) models. Frontiers in artificial intelligence and applications **155** (2007)
21. Guizzardi, G., Pires, L.F., Van Sinderen, M.: An ontology-based approach for evaluating the domain appropriateness and comprehensibility appropriateness of modeling languages. In: MoDELS. pp. 691–705. Springer (2005)
22. Hadar, E., Hassanzadeh, A.: Big data analytics on cyber attack graphs for prioritizing agile security requirements. In: 2019 IEEE 27th International Requirements Engineering Conference (RE). pp. 330–339. IEEE (2019)
23. Herre, H.: General formal ontology (gfo): A foundational ontology for conceptual modelling. In: Theory and applications of ontology: computer applications, pp. 297–345. Springer (2010)
24. Horrocks, I., et al.: Daml+oil: A description logic for the semantic web. IEEE Data Eng. Bull. **25**(1), 4–9 (2002)
25. Iannacone, M., Bohn, S., Nakamura, G., Gerth, J., Huffer, K., Bridges, R., Ferragut, E., Goodall, J.: Developing an ontology for cyber security knowledge graphs. In: 10th Annual Cyber and Information Security Research Conference (2015)
26. Jia, Y., Qi, Y., Shang, H., Jiang, R., Li, A.: A practical approach to constructing a knowledge graph for cybersecurity. Engineering **4**(1), 53–60 (2018)
27. Kang, D., Lee, J., Choi, S., Kim, K.: An ontology-based enterprise architecture. Expert Systems with Applications **37**(2), 1456–1464 (2010)
28. Keil, J.M., Schindler, S.: Comparison and evaluation of ontologies for units of measurement. Semantic Web **10**(1), 33–51 (2019)
29. Mascardi, V., Cordì, V., Rosso, P.: A comparison of upper ontologies. In: Woa. vol. 2007, pp. 55–64 (2007)
30. Mozzaquatro, B.A., Agostinho, C., Goncalves, D., Martins, J., Jardim-Goncalves, R.: An ontology-based cybersecurity framework for the internet of things. Sensors **18**(9), 3053 (2018)
31. Mundie, D.A., Ruefle, R., Dorofee, A.J., Perl, S.J., McCloud, J., Collins, M.: An incident management ontology. In: STIDS. pp. 62–71 (2014)
32. Narayanan, S., Ganesan, A., Joshi, K., Oates, T., Joshi, A., Finin, T.: Cognitive techniques for early detection of cybersecurity events. arXiv preprint arXiv:1808.00116 (2018)
33. Obrst, L., Chase, P., Markeloff, R.: Developing an ontology of the cyber security domain. In: STIDS. pp. 49–56 (2012)
34. Oltramari, A., Cranor, L.F., Walls, R.J., McDaniel, P.: Computational ontology of network operations. In: MILCOM 2015-2015 IEEE Military Communications Conference. pp. 318–323. IEEE (2015)
35. Oltramari, A., Cranor, L.F., Walls, R.J., McDaniel, P.D.: Building an ontology of cyber security. In: STIDS. pp. 54–61. Citeseer (2014)
36. Oltramari, A., Henshel, D.S., Cains, M., Hoffman, B.: Towards a human factors ontology for cyber security. In: STIDS. pp. 26–33 (2015)
37. Oltramari, A., Vetere, G., Lenzerini, M., Gangemi, A., Guarino, N.: Senso comune. In: LREC (2010)

38. Onwubiko, C.: 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 (2018)
39. Ou, X., Govindavajhala, S., Appel, A.W.: Mulval: A logic-based network security analyzer. In: USENIX security symposium. vol. 8, pp. 113–128. Baltimore (2005)
40. Parmelee, M.C.: Toward an ontology architecture for cyber-security standards. STIDS **713**, 116–123 (2010)
41. Pipa, A.M.C.: OWL ontology quality assessment and optimization in the cybersecurity domain. Ph.D. thesis, Instituto Universitário de Lisboa (2018)
42. Rose, S., Engel, D., Cramer, N., Cowley, W.: Automatic keyword extraction from individual documents. In: Berry, M.W., Kogan, J. (eds.) Text Mining. Applications and Theory, pp. 1–20. John Wiley and Sons, Ltd (2010)
43. Rutkowski, A., Kadobayashi, Y., Furey, I., Rajnovic, D., Martin, R., Takahashi, T., Schultz, C., Reid, G., Schudel, G., Hird, M., Adegbite, S.: Cybex: The cybersecurity information exchange framework (x.1500). SIGCOMM Comput. Commun. Rev. **40**(5), 59–64 (2010)
44. Sikos, L.F.: OWL Ontologies in Cybersecurity: Conceptual Modeling of Cyber-Knowledge, pp. 1–17. Springer International Publishing, Cham (2019)
45. Singhal, A., Ou, X.: Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs, pp. 53–73. Springer International Publishing (2017)
46. Syed, R., Zhong, H.: Cybersecurity vulnerability management: An ontology-based conceptual model (2018)
47. Syed, Z., Padia, A., Finin, T., Mathews, L., Joshi, A.: UCO: A unified cybersecurity ontology. In: Workshops at the Thirtieth AAAI Conference on Artificial Intelligence (2016)
48. Takahashi, T., Kadobayashi, Y.: Reference ontology for cybersecurity operational information. The Computer Journal **58**(10), 2297–2312 (2015)
49. Takahashi, T., Fujiwara, H., Kadobayashi, Y.: Building ontology of cybersecurity operational information. In: Proceedings of the Sixth Annual Workshop on Cyber Security and Information intelligence Research. pp. 1–4 (2010)
50. Takahashi, T., Kadobayashi, Y.: cybersecurity information exchange techniques: Cybersecurity information ontology and cybex. Journal of the National Institute of Information and Communications Technology Vol **58**(3/4) (2011)
51. Takahashi, T., Kadobayashi, Y., Fujiwara, H.: Ontological approach toward cybersecurity in cloud computing. In: Proceedings of the 3rd international conference on Security of information and networks. pp. 100–109 (2010)
52. Undercofer, J., Joshi, A., Finin, T., Pinkston, J., et al.: A target-centric ontology for intrusion detection. In: Workshop on Ontologies in Distributed Systems, held at The 18th International Joint Conference on Artificial Intelligence (2003)
53. Wand, Y., Weber, R.: On the deep structure of information systems. Information Systems Journal **5**(3), 203–223 (1995)
54. Wang, J.Z., Ali, F.: An efficient ontology comparison tool for semantic web applications. In: The 2005 IEEE/WIC/ACM International Conference on Web Intelligence (WI'05). pp. 372–378. IEEE (2005)
55. Wang, J.A., Guo, M.: 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 (2009)
56. Wieringa, R.: Design Science Methodology for Information Systems and Software Engineering. Springer (2014)
57. Zuanelli, E.: The cybersecurity ontology platform: the poc solution. e-AGE2017 p. 1 (2017)