COMPUTACION E INFORMATICA

Recibido *04/03/2021* ***ReCIBE, Año 9 No. 2, Noviembre 2020***

Aceptado *05/03/2021*

Cybersecurity Ontologies: A Systematic Literature Review

Revisión sistemática de la literatura sobreontologías en ciberseguridad

William Fernando Borja Rivadeneira[2]
william.f.borja.r@pucesa.edu.ec

Omar S. Gómez[1,2]
ogomez@espoch.edu.ec

[1]GrIISoft Research Group, Escuela Superior Politécnica de Chimborazo, Riobamba,Ecuador.

[2]Pontificia Universidad Católica del Ecuador Sede Ambato, Ambato, Ecuador

Abstract: Cybersecurity is a young discipline that has gained relevance in our modern society. This research reports the findings of a systematic review of the literature on ontologies in the field of cybersecurity. From an initial set of 214 papers on the subject, 50 relevant papers were selected for this SLR. With these documents we answered research questions related to the domains in which ontologies are reported, the methodologies, tools and languages used, and the verification and validation mechanisms reported. As results, we observed that the largest number of ontologies are classified in the domains of infrastructure and networking, software and human factor. Regarding the papers that report the use of a methodology for developing the ontologies (12%), Methontology is the commonly used one. Protégé, in conjunction with the OWL language, are the preferred tools for ontology development. Regarding verification and validation (V&V) mechanisms, we observe that more than half (62%) report the application of V&V mechanisms to their ontologies.

Keywords: Systematic Literature Review, Ontology, Cyber-security, Cybersecurity Ontologies, ICT.

Resumen: La ciberseguridad es una disciplina joven que ha tomado relevancia en nuestra sociedad moderna. En la presente investigación se reportan los hallazgos de una revisión sistemática de la literatura sobre ontologías en el ámbito de la ciberseguridad. De un conjunto inicial de 214 documentos sobre el tema, para la presente SLR se utilizaron 50 documentos relevantes. Con estos documentos se respondieron preguntas de investigación relacionadas con los dominios en los que se reportan las ontologías, las metodologías, herramientas y lenguajes usados, así como los mecanismos de verificación y validación reportados. Con respecto a los resultados observamos que el mayor número de ontologías se clasifican en los dominios de infraestructura y networking, software y factor humano, dentro del porcentaje de documentos en los que se reporta el uso de alguna metodología para el desarrollo de ontologías (12%), methontology es la metodología comúnmente usada. Protege en conjunto con el lenguaje OWL es la herramienta de preferencia para el desarrollo de ontologías. En cuando a los mecanismos de verificación y validación, observamos que poco más de la mitad (62%) reporta algún mecanismo de V&V.

Palabras Claves: Revisión Sistemática de la Literatura, Ontología, Ciber-seguridad, Ontologías de Ciberseguridad, ICT.

INTRODUCTION

There is no doubt that Information and Communications Technology (ICT) has significantly revolutionized the knowledge society in which we are immersed. Advances in software, hardware and telecommunications have managed to converge in different sectors of our society, offering modern solutions. However, due to the massification of TICs, issues related to vulnerabilities and threats in software, hardware and telecommunications have arisen.

Cybersecurity is a young discipline aimed at protecting vulnerabilities or minimizing threats to technological infrastructure such as software, hardware and telecommunications (Thakur and Pathan, 2014). Although knowledge about cybersecurity issues is mostly held by people involved in the ICT arena, due to massive use of ICT, knowledge about cybersecurity should be extended to the general public (Singer and Friedman, 2014).

Knowledge about cybersecurity has been gradually built up thanks to the diversity of contributions made by different experts in this field. A portion of these contributions have focused on creating ontologies that help to define, represent and organize a vocabulary of concepts (Neches et al., 1991) related to this discipline. These ontologies provide a shared knowledge on the different aspects of cybersecurity. In order to have a better understanding of ontologies reported in the field of cybersecurity, this paper presents the results of a systematic review of the literature on the various ontologies that have been reported in the context of cybersecurity.

The rest of the document is organized as follows: Section II presents some generalities about ontologies; Section III describes the method used in which the research questions to be answered by this systematic review are framed. Section IV presents the results with respect to the specified research questions. Finally, section V discusses the results and presents the conclusions.

ONTOLOGIES

In the origins of Western thought, ontology was considered a discipline related to philosophy. It was oriented to the study of the existing (entities) and their relationships. In a general way, an ontology can be defined as a vocabulary, in which entities, classes, properties, predicates, functions and the relations between these elements are stated. An ontology is important because it enables sharing knowledge regarding a particular domain.

In the literature we can find different approaches or methods to create ontologies (Lenat and Guha, 1990; Uschold and King, 1995; Grüninger and Fox, 1995; Bernaras et al., 1996; Fernandez et al., 1997; Swartout et al., 1997; Staab et al., 2001; KBSI, 1994). For example, in (Lenat and Guha 1990) authors propose an approach for the creation of ontologies that support intelligent systems based on knowledge. Similarly, in (Uschold and King, 1995) authors propose an ontology construction method aimed at capturing knowledge, coding it and integrating it with existing ontologies. In the case of (Grüninger and Fox, 1995), authors propose a methodology that allows the development of systems based on first-order knowledge; in addition, taking advantage of the robustness of classical logic as a guide to transform informal systems into computational ones.

This methodology focuses on identifying the main scenario for the construction of ontologies. On the other hand, in (Bernaras et al., 1996), the Kactus methodology is presented. It focuses on the construction of ontologies considering a knowledge base that uses a process of abstraction, where the context of the entities is specified. One of the widely known methodology is Methontology, proposed by Juristo (Fernandez et al., 1997). It helps to create a new ontology as well as reusing existing ones. This methodology fits into a development process based on the creation of prototypes.

The SENSUS method (Swartout et al., 1997) is another approach, it uses existing ontologies creating an ontology skeleton, the resulting prototype eliminates terms irrelevant to the domain knowledge. Another methodology is Onto-Knowledge (Staab et al., 2001), a project that supports the development of ontologies for knowledge management. Finally, in (KBSI, 1994), authors mention the KBSI IDEF5 method, which is a method that allows and helps in the creation, modification and maintenance of ontologies.

Tools are also relevant in developing ontologies. Examples of these tools are: Ontolingua Server (Farquhar et al., 1997), Ontosaurus (Swartout et al., 1997), Protégé (Noy et al., 2000), WebODE (Arpírez et al., 2003), OntoEdit (Sure et al., 2002), among others. One tool that is commonly used in the creation of ontologies is Protégé (Noy et al., 2000), which is an independent open-source tool that has an extensible architecture. Its main core is the ontology editor, that its functionality can be extended through the use of plug-ins.

Another tool that supports the creation of ontologies is Ontosaurus (Swartout et al., 1997). It consists of two modules: an ontology server that uses a knowledge representation system and a web browser that allows editing and exploring ontologies using HTML. It is worth to note that several of these tools have their own ontology development language. Examples of these languages are: XOL (XML-Based Ontology Exchange Language) (Karp et al., 1999); SHOE (Simple HTML Ontology Extensions) (Luke and Heflin, 2000); which is an extension of HTML, DAML+OIL (Horrocks and van Harmelen, 2001) and OWL (Web Ontology Language) (Dean and Schreiber,2003).

These languages vary according to their use; besides considering that these languages can be integrated through extensions or APIs established by the provider of these languages. OWL (Dean and Schreiber, 2003) is one of the languages commonly used by ontology developers. OWL is aimed at publishing and sharing ontologies developed on the Web. OWL is a derivation of DAML+OIL (Horrocks and van Harmelen, 2001) which shares some of its functionalities.

When an ontology is developed, an important aspect to take into account is the one related to their verification and validation (V&V) (Raad and Cruz, 2015). It can be approached from two perspectives: with regards to its quality and with regards to its correctness (Raad and Cruz, 2015). In the literature we can find some approaches that address the verification and validation of an ontology, such as: the gold standard approach (Ulanov et al., 2010); corpus-based (Brewster et al., 2004); task-based (Welty et al., 2003) and criteria-based (Fernandez et al., 2009). As for the gold standard approach (Ulanov et al., 2010), it focuses on comparing the developed ontology with a reference ontology created with certain criteria.

On the other hand, the corpus-based approach (Brewster et al., 2004), consists in evaluating the coverage of an ontology with one or several ontologies through a corpus in which the determined domain is significantly covered. In the case of the task-based approach (Welty et al., 2003), the evaluation of an ontology is aimed at a specific task, based on the results obtained to improve the knowledge of this task. Another approach consists in validating the ontology according to a desirable criterion (Raad and Cruz, 2015), such as its structure (Fernandez et al., 2009), where for example the number of nodes that an ontology has is used, or more complex criteria may be used.

Another approach is based on experts (Alani and Brewster, 2006), for example, evaluations are based on the coincidences of classes, density and intermediation that are detailed in the ontology. Some support tools for V&V tasks are OntoMetric (Lozano et al., 2004), natural language application metrics (Hartmann et al., 2004), OntoClean (Gangemi et al., 2002); EvaLexon (Spyns et al., 2004) and OOPS! (Poveda et al., 2015). For example, OntoClean (Gangemi et al., 2002), allows the evaluation of an ontology based on its taxonomic structure. Another case is OOPS! (Poveda et al., 2015), a tool that scans an ontology by using a URL to find possible inconsistencies that may affect the modeling of it.

METHOD

The guideline described in (Kitchenham, 2004) was followed in order to conduct the Systematic Literature Review (SLR) here reported. According to (Kitchenham, 2004), the realization of a SLR is divided into three phases: planning, execution and reporting, following we describe each of these phases in our context.
As part of the planning phase, the protocol for this SLR was developed. It sets out the research questions, as well as the objectives of this research. In this phase, the source for searching, the search string, and the inclusion and exclusion criteria are also defined. In the second phase (execution) the protocol is run, in this phase we proceed with the searches of documents with respect to the search string defined in the protocol, we also carry out the discrimination of the documents according to the inclusion and exclusion criteria defined in the protocol, we also carry out the analysis and synthesis of the relevant documents (selected papers). Finally, the third phase corresponds to the presentation of the results of this SLR.

The main objective of this SLR is to gain a better understanding of reported ontologies related to cybersecurity domain. With respect to this objective, the following research questions have been posed.

- RQ1. What areas of cybersecurity are the ontologies reported in?
- RQ2. What methods or approaches have been used for the development of the selected ontologies?
- RQ3. What tools have been used for the construction of the reported ontologies?
- RQ4. Have the reported ontologies been validated?

Identification and selection of the searching source

For the present work, the Scopus database has been chosen. It contains the largest number of abstracts and citations in the scientific literature as well as offers a search engine with advanced searching options.

Definition of the search string

The search string has been defined with different terms based on the subject matter of this SLR, these terms have been combined with logical operators, resulting in the following search string:

TITLE-KEY-ABS(ontology AND (cyber-security OR cybersecurity OR “cyber security”))

Inclusion Criteria(CI) and Exclusion Criteria (CE)

We filtered the selection of primary studies (documents on the subject) in terms of the following inclusion and exclusion criteria. The primary studies were selected based on the title, abstract and keywords in order to determine whether they are identified as relevant ones, documents were selected taking into account compliance with the following inclusion criteria: papers reporting cybersecurity ontologies written in English language. These papers should be published in prestigious indexed venues such as journals, proceedings and book chapters subject to a peer review process. In the same way, those papers that met some of the following exclusion criteria were not considered for this SLR: duplicated papers, papers whose main contribution is not related with cybersecurity ontologies, poster papers, non-English written papers, and short communications such as letters to the editor.

Execution

Once the protocol was defined, we proceeded with the execution phase. The previously defined search string was executed in September 2020, using the Scopus database search engine. It is worth to note that Scopus is one of the biggest abstract and citation database in the arena of scientific literature. Initially 214 document results were obtained after running the search string. After applying the inclusion and exclusion criteria on titles, abstracts and keywords, 72 documents were selected (first filter).

From this selection, the complete content of 69 documents was accessed. After analyzing the content of these documents, 19 were discarded, so finally 50 documents were considered for this review (relevant papers). According to the previously described, we used the Scopus database to run the search string, and the contents of the relevant documents was accessed through their respective publishers such as IEEE, Springer, ACM, Science Direct, among others.

As shown in Figure 1, the first ontology related to cybersecurity was reported in 2004 (Simmonds et al., 2004), from that year onwards, other works sporadically arise, it is from 2014 that the number of ontologies related to cybersecurity increases, for example in 2019 eleven ontologies were reported (Burita, 2019; Vega Barbas et al., 2019; Gasmi et al., 2019; Doynikova et al., 2019; Scarpato et al., 2019; Niyazova et al., 2019; Islam et al., 2019; Baesso Moreira et al., 2019; Katsantonis et al., 2019; Shaaban et al., 2019; Zamfira et al., 2019).

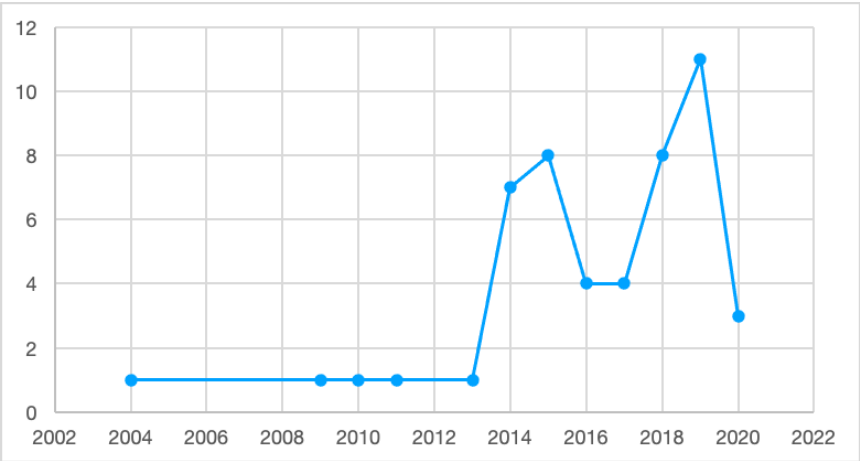

Figure 1. Chronology of ontologies reported in the context of cybersecurity.

It is worth to note that the relevant papers used in this SLR were subjected to a quality assessment. Nine evaluation criteria adapted from (Kitchenham, 2004) were considered, these criteria are related to the year of publication, the type of publication (journal or conference) as well as criteria related to the structure of the selected documents. A Likert scale was used for this purpose, where the maximum evaluation score was set 50 points, Table 1 shows the nine criteria used for the assessment.

TABLE 1. Quality assessment criteria used for this SLR.

The authors of this paper carried out the evaluation of the relevant documents and the results of the evaluation were averaged. As can be seen in Table 2, none of the papers was rejected based on the evaluation criteria used.

Quality percentage score by category	Number of papers	Percentage of papers
Poor (<26%)	0	0%
Regular (26%-45%)	0	0%
Good (46%-65%)	19	38%
Very Good (66%-85%)	26	52%
Excellent (>86%)	5	10%

TABLE 2. Quality assessment outcome.

The total score from each paper was computed using a percentage scale. We observe that all of the relevant papers yielded a quality score that ranges from good to excellent. The average score of this evaluation was 76%, which was considered a good enough quality indicator for this SLR.

RESULTS

This section presents the results of the information synthesis process. These results are structured with respect to the research questions stated for this SLR.

RQ1. What areas of cybersecurity are the ontologies reported in?

Regarding this research question, we have identified four categories in which the ontologies are grouped: General, Networking, Software and Human Factor. The general category refers to those ontologies that involve a mix of concepts related to the other categories, such as networking, software, or the human factor. In the category of networking the ontologies address concepts related to equipment, protocols and network modeling. In the software category, the ontologies are mainly focused on describing cybersecurity concepts from a software development perspective. In the category of human factor are those ontologies that describe concepts related to the personnel involved in aspects of cybersecurity in ICTs. Table 3 presents the ontologies grouped by the categories previously described. As shown in Table 3, the largest number of ontologies analyzed are grouped in the general and networking categories.

Scope / Domain	*Number of papers*	*Percentage of papers*	*References*
General	17	34%	Burita (2019), Vega Barbas et al. (2019), Doynikova et al. (2019), Baesso Moreira et al. (2019), Onwubiko et al. (2018), Zhao et al. (2018), Petrenko and Makoveichuk, (2017), Elnagdy et al. (2016), Falk (2016), Maines et al. (2015), Gcaza et al. (2015), Salem and Wacek (2015), Oltramari et al. (2014), Geller et al. (2014), Van Vuuren et al. (2014), Obrst et al. (2014), Wali et al. (2013)
Networking	16	32%	Chukkapalli et al. (2020), Scarpato et al. (2019), Katsantonis et al. (2019), Shaaban et al. (2019), Zamfira et al. (2019), Zamfira et al. (2018), Mozzaquatro et al. (2018), Zheng et al. (2018), Albalushi et al. (2018), Bergner and Lechner (2017), Oltramari et al., (2015), Iannacone et al. (2015), Laskey et al. (2015), Takahashi et al. (2010), Hieb et al. (2009), Simmonds et al. (2004)
Software	9	18%	Syed (2020), Bataityte et al. (2020), Gasmi et al. (2019), Islam et al. (2019), Ochoa et al. (2018), Alqahtani and Rilling (2017), Syed et al. (2016) Huang et al. (2014), Razzaq et al. (2014)
Human Factor	8	16%	Niyazova et al. (2019), Maathuis et al. (2018), Tseng et al. (2017), Fontenele and Sun (2016), Oltramari et al. (2015), Chun and Geller (2015), Takahashi and Kadobayashi (2014), Takahashi and Kadobayashi (2011)

TABLE 3. Classification of Ontologies according to their scope.

RQ2. What methods or approaches have been used for the development of the selected ontologies?

Regarding this research question, we observe that most of the authors of the reported ontologies (88%,44 papers) do not mention to use existing methods for the development of their ontologies. In other words, the authors describe their own approach that they followed for the development of their ontologies. To a lesser extent we observe that only in six relevant papers (12%), the authors mention following some existing methodology for the development of their ontologies. For example, four authors mention the use of the Methontology methodology (Fernandez et al., 1997), while two authors mention the use of the methodology Ontology Development 101 (Noy and McGuinness, 2001).

Table 4 shows the resulting classification with regards this research question.

Existing Method	***Number of papers***	***Percentage of papers***	***References***
Without Following Existing Methods	44	88%	Syed (2020), Chukkapalli et al. (2020), Bataityte et al. (2020), Burita (2019), Vega Barbas et al. (2019), Gasmi et al. (2019), Doynikova et al. (2019), Scarpato et al. (2019), Niyazova et al. (2019), Islam et al. (2019), Baesso Moreira et al. (2019), Shaaban et al. (2019), Onwubiko et al. (2018), Zamfira et al. (2018), Mozzaquatro et al. (2018), Zheng et al. (2018), Ochoa et al. (2018), Zhao et al. (2018), Albalushi et al. (2018), Alqahtani and Rilling (2017), Tseng et al. (2017), Petrenko and Makoveichuk (2017), Bergner and Lechner (2017), Bergner and Lechner (2017), Fontenele and Sun (2016), Falk (2016), Syed et al. (2016), Maines et al. (2015), Oltramari et al. (2015), Iannacone et al. (2015), Gcaza et al. (2015), Oltramari et al. (2015), Salem and Wacek (2015), Chun and Geller (2015), Laskey et al. (2015), Oltramari et al. (2014), Geller et al. (2014), Takahashi and Kadobayashi (2014), Huang et al. (2014), Wali et al. (2013), Takahashi and Kadobayashi, (2011), Takahashi et al. (2010), Hieb et al. (2009) Simmonds et al. (2004)
Following Existing Methods	6	12%	Zamfira et al. (2019), Maathuis et al. (2018), Obrst et al. (2014), Razzaq et al. (2014), Katsantonis et al. (2019), Van Vuuren et al. (2014)

TABLE 4. Classification of Ontologies according to their methodology.

As shown in Table 4, only six papers report the use of a methodology for developing their ontologies. Methontology approach was reported in four papers (Zamfira et al., 2019; Maathuis et al., 2018; Obrst et al., 2014; Razzaq et al., 2014), whereas the ontology development 101 method was reported in two works (Katsantonis et al.,2019; Van Vuuren et al., 2014).

RQ3.What tools have been used for the construction of the reported ontologies?

In the case of the tools that support the construction of ontologies, 40% of the documents (20 papers) authors mention the use of some tool to support the development of their ontologies. We observe that Protégé is the most used tool for ontology development; its use is mentioned in 16 out of 20 relevant documents that mention the use of a tool. To a lesser extent, the use of other tools is also reported, such as Atom-Tool; Cyber Security Ontology Expert Tool; CYBEX; and IntelMQ. Table 5 shows the ontologies grouped by tools.

Tool	Number of papers	Percentage of papers	References
Protégé	16	32%	Syed (2020), Bataityte et al. (2020), (2019), Katsantonis et al. (201 (2019), Zamfira et al. (2018 (2018), Ochoa et al. (20 Oltramari et al. (201 et al. (2014), (2014), Ra
ATOM-TOOL	1	2%	
Cyber Security Ontology Expert Tool	1		
CYBEX			
IntelM			

TABLE 5. Ontology classification by used tools

The tools used for the ontology development usually incorporate languages that help in the definition of ontologies. We observe that 24% (12 papers) of the relevant documents (Chukkapalli et al., 2020; Vega Barbas et al., 2019; Doynikova et al., 2019; Zheng et al., 2018; Petrenko and Makoveichuk, 2017; Elnagdy et al., 2016; Falk, 2016; Syed et al., 2016; Iannacone et al., 2015; Oltramari et al., 2015; Salem and Wacek, 2015; Laskey et al., 2015) report the use of the OWL language (Dean and Schreiber, 2003).

To a lesser extent, the use of languages such as SPARQL, SWRL, XML and OWL 2 is observed (Baesso Moreira et al., 2019; Onwubiko et al., 2018; Albalushi et al., 2018; Tseng et al., 2017; Bergner and Lechner, 2017; Fontenele and Sun, 2016; Maines et al., 2015; Geller et al., 2014).

RQ4. Have the reported ontologies been validated?

Regarding the evaluation and validation of the ontologies reported in this SLR, we observe that 62% of them (31 primary studies) mention the use of some verification or validation mechanisms. For example, in 18 relevant papers, authors mention the use of information extraction rules similar to those proposed in (Boley et al., 2001). In the case of the ontologies here reported, some authors perform the verification and validation of their ontologies based on the comparison with existing ontologies (3 relevant papers). Another type of validation observed is the validation by experts, approach mentioned in other three relevant papers. The use of tools for assessing ontologies is also mentioned, tools like OntoClean (Gangemi et al., 2002), the OQuare metrics tool (Duque and Fernandez, 2011), and a Protégé extension called HermiT Reasoner (Data and Knowledge Group) are mentioned. We also observe hybrid approaches in which validation is conducted through the use of criteria (Fernandez et al., 2009) and tasks (Welty et al., 2003). Finally, we also observe the use of a metrics-based validation approach. Table 6 shows the resulting classification regarding this research question.

Evaluation / Validation	*Number of papers*	*Percentage of papers*	*References*
Information Extraction Rules	18	36%	Islam et al. (2019), Baesso Moreira et al. (2019), Katsantonis et al. (2019), Shaaban et al. (2019), Ochoa et al. (2018), Zhao et al. (2018), Alqahtani and Rilling (2017), Tseng et al. (2017), Petrenko and Makoveichuk (2017) Elnagdy et al. (2016), Falk (2016), Maines et al. (2015), Salem and Wacek (2015), Laskey et al. (2015), Geller et al. (2014), Takahashi and Kadobayashi (2014), Huang et al. (2014), Takahashi and Kadobayashi (2011)
Comparison with Existing Ontologies	3	6%	Zheng et al. (2018), Syed et al. (2016), Iannacone et al. (2015)
Experts' validation	3	6%	Fontenele and Sun (2016), Chun and Geller (2015), Wali et al. (2013)
OntoClean	3	6%	Zamfira et al. (2019), Zamfira et al. (2018), Razzaq et al. (2014)
OQuare metrics	1	2%	Mozzaquatro et al. (2018)
HermiT Reasoner	1	2%	Maathuis et al. (2018)
Hybrid Approach	1	2%	Syed (2020)
Metrics-based Validation	1	2%	Gasmi et al. (2019)

TABLE 6. Evaluation and validation approaches reported.

DISCUSSION AND CONCLUSIONS

The highest percentage of ontologies reported in the field of cybersecurity are in the general and networking category. The general category addresses a mix of concepts belonging to the networking, software and human factor categories. These findings suggest that work is being done on the definition of ontologies in specific cybersecurity domains. However, we also observe work on the development of ontologies addressing a more general domain of the cybersecurity.

Regarding the methods or approaches used for the development of ontologies, we observe that in most of the relevant documents analyzed, authors do not mention following existing methodologies for developing their ontologies. Only in 12% (six papers) authors mention using some methodology as a reference. From this percentage, the most used methodology is Methontology (Fernandez et al., 1997). These findings seem to suggest a lack of motivation in the use of existing ontology development methodologies. We observe that the most widely used tool for the construction of ontologies is Protégé (Noy et al., 2000).
From the ontologies that report the use of some tool, 32% (16 papers) report the use of Protégé. OWL (Dean and Schreiber, 2003) is the most used language among the ontologies that report the use of a language.

Finally, regarding the use of verification and validation (V&V) mechanisms, we observe that 62% of the primary studies report the use of some verification or validation mechanism, among which the following stand out: the use of information extraction rules, making of comparisons with respect to existing ontologies, validation by experts, validation through the use of metrics, as well as the use of tools for this purpose. We observe that gradually there is interest in applying V&V mechanisms that help to correct deficiencies in the development of ontologies in the field of cybersecurity.

Study Limitations

It is worth to note that secondary studies as the one here reported are subject to interpretation in its different phases, thus implying the presence of bias. In order to minimize a possible bias, we followed the main phases with its activities of the SLR methodology. Although the risk of missing relevant papers was present, we consider that the selected documents for this review (relevant papers) represent a good enough sample of reported cybersecurity ontologies.

In this SLR, we did not consider gray literature, so we assume that good quality grey literature of this subject will be reported in journals or conferences, because of this, possible publication bias may arise due to negative findings are not usually published. We did not consider documents published in a non-English language, although this is not a limitation in our regional context, it can be a reflection of the limitations imposed on us by the available research in this area (updated and peer-reviewed literature is commonly published in English).

Cybersecurity is a young discipline in which disciplines such as telecommunications, electronics and computing have converged. The arrival of different ontologies in the field of cybersecurity has fostered to have more knowledge of the concepts related to this discipline. In this research we have reported the results of a systematic literature review on cybersecurity ontologies. The main contribution of this secondary study is the synthesis of the findings from the different ontologies reported with respect to areas or domains, methodologies, tools and languages used, as well as the V&V mechanisms reported. The results of our work can serve as a reference for future research on this topic.

REFERENCES

Alani, H. and Brewster, C. (2006). Metrics for ranking ontologies.

Albalushi, A., Khan, R., McLaughlin, K. and Sezer, S. (2018). Ontology-based approach for malicious behaviour detection in synchrophasor networks. IEEE Power and Energy Society General Meeting, 1-5.

Alqahtani, S. S. and Rilling, J. (2017). An Ontology-Based Approach to Automate Tagging of Software Artifacts. International Symposium on Empirical Software Engineering and Measurement, 169174.

Arpírez, J., Corcho, O., Fernandez, M. and Gómez, A. (2003). WebODE in a nutshell. AI Magazine.

Baesso Moreira, G., Menditi Calegario, V., Duarte, J. C. and Pereira, Dos Santos, A. F. (2019). Extending the VERIS Framework to an Incident Handling Ontology. 2018 IEEE/WIC/ACM International Conference on Web Intelligence, 8609628, 440-445.

Bataityte, K., Vassilev, V. and Gill, O.J. (2020). Ontological foundations of modelling security policies for logical analytics. IFIP Advances in Information and Communication Technology, 583, 368380.

Bergner, S. and Lechner, U. (2017). Cybersecurity ontology for critical infrastructures. 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, 2, 80-85.

Bernaras, A., Laresgoiti, I. and Corera, J. (1996). Building and reusing ontologies for electrical network applications. Wahlster W (ed) European Conference on Artificial Intelligence (ECAI'96), 298– 302.

Boley, H., Tabet, S. and Wagner, G. (2001). Design Rationale of RuleML: A Markup Language for Semantic Web Rules. In the first Semantic Web Working Symposium.

Brewster, C., Alani, H., Dasmahapatra, S. and Wilks, Y. (2004). Data driven ontology evaluation.

Burita, L. (2019). Model of a Vocabulary. Frontiers in Artificial Intelligence and Applications, 321, 8391.

Chukkapalli, S. S. L., Piplai, A., Mittal, S., Gupta, M. and Joshi, A. (2020). A Smart-Farming Ontology for Attribute Based Access Control. 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, 9123052, 29-34.

Chun, S.A. and Geller, J. (2015). Developing a pedagogical cybersecurity ontology. Communications in Computer and Information Science, 178, 117-135.

Data and Knowledge Group. HermiT OWL Reasoner: The New Kid on the OWL Block. Department of Computer Science, University of Oxford, http://www.hermit-reasoner.com/

Dean, M. and Schreiber, G. (2003). OWL Web Ontology Language Reference. http://www.w3.org/TR/owl-ref/

Doynikova, E., Fedorchenko, A. and Kotenko, I. (2019). Ontology of metrics for cyber security assessment. ACM International Conference Proceeding Series, 3341496.

Duque, A. and Fernandez, J. (2011). OQuaRE: A SQuaRE-based Approach for Evaluating the Quality of Ontologies. Journal of Research and Practice in Information Technology.

Elnagdy, S.A., Qiu, M. and Gai, K. (2016). Cyber Incident Classifications Using Ontology-Based Knowledge Representation for Cybersecurity Insurance in Financial Industry. 3rd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2016 and 2nd IEEE International Conference of Scalable and Smart Cloud, SSC 2016, 7545936, 301-306.

Falk, C. (2016). An ontology for threat intelligence. European Conference on Information Warfare and Security, ECCWS, 111-116.

Farquhar, A., Fikes, R. and Rice, J. (1997). The Ontolingua Server: A Tool for Collaborative Ontology Construction. International Journal of Human Computer Studies, 46(6), 707–727.

Fernandez, M., Gomez, A. and Juristo, N. (1997). METHONTOLOGY: From Ontological Art Towards Ontological Engineering. Spring Symposium on Ontological Engineering of AAAI, 33-40.

Fernandez, M., Overbeeke, C., Sabou, M. and Motta, E. (2009). What makes a good ontology? A casestudy in fine-grained knowledge reuse. The semantic web, Springer, 61-75.

Fontenele, M. and Sun, L. (2016). Knowledge management of cyber security expertise: An ontological approach to talent discovery. 2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016, 7502356.

Gangemi, A., Guarino, N., Oltramari, A. and Borgo, S. (2002). Cleaning-up WordNet's Top- Level. 1st International WordNet Conference.

Gasmi, H., Laval, J. and Bouras, A. (2019). Cold-start cybersecurity ontology population using information extraction with LSTM. 2019 International Conference on Cyber Security for Emerging Technologies, 8904905.

Gcaza, N., Von, Solms, R. and Van, Vuuren, J. (2015). An ontology for a national cyber-security culture environment. 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 1-10.

Geller, J., Ae Chun, S. and Wali, A. (2014). A hybrid approach to developing a cyber security ontology. 3rd International Conference on Data Management Technologies and Applications, 377-384.

Grüninger, M. and Fox, M. (1995). Methodology for the design and evaluation of ontologies. Skuce D

(eds) IJCAI'95 Workshop on Basic Ontological Issues in Knowledge Sharing, 6.1-6.10.

Hartmann, J., Spyns, P., Giboin, A., Maynard, D., Cuel, R., Carmen, M. and Sure, Y. (2004). Methods for ontology evaluation. Knowledge Web Deliverable D1.2.3, 1.

Hieb, J., Graham, J. and Guan, J. (2009). An ontology for identifying cyber intrusion induced faults in process control systems. IFIP Advances in Information and Communication Technology, 311, 125-138.

Horrocks, I. and van Harmelen F. (2001). Reference Description of the DAML+OIL (March 2001) Ontology Markup Language. http://www.daml.org/2001/03/reference.html

Huang, H., Lee, C., Wang, M. and Kao, H. (2014). IT2FS-based ontology with soft-computing mechanism for malware behavior analysis. Soft Computing, 18, 267-284.

Iannacone, M., Bohn, S., Nakamura, G., Gerth, J., Huffer, K., Bridges, R., Ferragut, E. and Goodall, J. (2015). Developing an ontology for cyber security knowledge graphs. ACM International Conference, 12.

Islam, C., Babar, M.A. and Nepal, S. (2019). An ontology-driven approach to automating the process of integrating security software systems. 2019 IEEE/ACM International Conference on Software and System Processes, 8812856, 54-63.

Karp, P., Chaudhri, V. and Thomere, J. (1999). XOL: An XML-Based Ontology Exchange Language. http://www.ai.sri.com/~pkarp/xol/xol.html

Katsantonis, M. and Mavridis, I. (2019). Ontology-Based Modelling for Cyber Security E-Learning and Training. Computer Science, 11841, 15-27.

KBSI (1994). The IDEF5 Ontology Description Capture Method Overview. KBSI Report.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. Software Engineering Group Department of Computer Science.

Laskey, K. B., Chandekar, S. and Paris, B. (2015). A probabilistic ontology for large-scale IP geolocation. CEUR Workshop, 1523, 18-25.

Lenat, D. and Guha, R. (1990). Building Large Knowledge-based Systems: Representation and Inference in the Cyc Project. Addison-Wesley

Lozano, A. and Gómez, A. (2004). ONTOMETRIC: A Method to Choose the Appropriate Ontology. Journal of Database Management. Special Issue on Ontological analysis, Evaluation and Engineering of Business Systems Analysis Methods, 15.

Luke, S. and Heflin, J. (2000). SHOE 1.01. Proposed Specification. Technical Report. Parallel Understanding Systems Group. http://www.cs.umd.edu/projects/plus/SHOE/spec1.01.htm

Maathuis, C., Pieters, W. and Van, Den, Berg, J. (2018). A computational ontology for cyber operations.

European Conference on Information Warfare and Security, ECCWS, 278-287.

Maines, C. L., Llewellyn Jones, D., Tang, S. and Zhou, B. (2015). A cyber security ontology for BPMNsecurity extensions. 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015, 7363310, 1756-1763.

Mozzaquatro, B.A., Agostinho, C., Goncalves, D., Martins, J. and Jardim-Goncalves, R. (2018). An ontology-based cybersecurity framework for the internet of things. Sensors, 18(3053).

Neches, R., Fikes, R. E., Finin T., Gruber, T. R., Senator, T. and Swartout, W. R. (1991). Enabling technology for knowledge sharing. AI Magazine, 12(3), 36-56.

Niyazova, R., Aktayeva, Al. and Davletkireeva, L. (2019). An Ontology based Model for User Profile building using Social Network. ACM International Conference Proceeding Series, 21.

Noy, N. F. and McGuinness, D. L. (2001). Ontology development 101: A guide to creating your first ontology. Stanford knowledge systems laboratory technical report KSL-01-05 and Stanford medical informatics technical report.

Noy, N., Fergerson, R. and Musen, M. (2000). The knowledge model of Protege-2000: Combining interoperability and flexibility. Springer-Verlag, 17–32.

Obrst, L., Chase, P. and Markeloff, R. (2014). Developing an ontology of the cyber security domain. CEUR Workshop, 966, 49-56.

Ochoa, O., Steinmann, J. and Lischuk, Y. (2018). Towards eliciting and analyzing security requirements using ontologies through use case scenarios (work-in-progress). 2018 4th International Conference on Software Security and Assurance, ICSSA 2018, 9092285, 1-6.

Oltramari, A., Cranor, L. F., Walls, R. J. and McDaniel, P. (2014). Building an ontology of cyber security. CEUR Workshop, 1304, 54-61.

Oltramari, A., Cranor, L. F., Walls, R. J. and McDaniel, P. (2015). Computational ontology of network operations. IEEE Military Communications Conference MILCOM, 7357462, 318-323.

Oltramari, A., Henshel, D., Cains, M. and Hoffman, B. (2015). Towards a human factors ontology for cyber security. CEUR Workshop, 1523, 26-33.

Onwubiko, C. (2018). CoCoa: An ontology for cybersecurity operations centre analysis process. 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018, 8551486.

Petrenko, S. A. and Makoveichuk, K. A. (2017). Ontology of cyber security of self-recovering smart Grid. CEUR Workshop, 2081, 98-106.

Poveda, M., Suárez M. C. and Gómez, A. (2015). Did You Validate Your Ontology? OOPS!. ESWC 2012 Satellite Events, 402–407.

Raad, J. and Cruz, C. (2015). A Survey on Ontology Evaluation Methods. Proceedings of the International Conference on Knowledge Engineering and Ontology Development, part of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management.

Razzaq, A., Anwar, Z., Ahmad, H. F., Latif, K. and Munir, F. (2014). Ontology for attack detection: An intelligent approach to web application security. Computers and Security, 45, 124-146.

Salem, M. B. and Wacek, C. (2015). Enabling new technologies for cyber security defense with the ICAS cyber security ontology. CEUR Workshop, 1523, 42-49.

Scarpato, N., Cilia, N.D. and Romano, M. (2019). Reachability Matrix Ontology: A Cybersecurity Ontology. Applied Artificial Intelligence, 33, 643-655.

Shaaban, A. M., Schmittner, C. and Gruber, T. (2019). Tackling the challenges of IoT security testing using ontologies. IDIMT 2019: Innovation and Transformation in a Digital World - 27th Interdisciplinary Information Management Talks, 411-418.

Simmonds, A., Sandilands, P. and Van Ekert, L. (2004). An ontology for network security attacks. Computer Science, 3285, 317-323.

Singer, P. W. and Friedman, A. (2014). Cybersecurity and Cyberwar What Everyone Needs to Know. Oxford University Press

Spyns, P., Pretorius, A. and Reinberger, M. (2004). Evaluating DOGMA-lexons generated automatically from a text corpus. Proceedings of the EKAW 2004 Workshop on Language and Semantic Technologies to support Knowledge Management Processes, 38 – 44.

Staab, S., Schnurr, H., Studer, R. and Sure, Y. (2001). Knowledge Processes and Ontologies. IEEE Intelligent Systems, 16(1), 26–34.

Sure, Y., Erdmann, M., Angele, J., Staab, S., Studer, R. and Wenke, D. (2002). OntoEdit: Collaborative Ontology Engineering for the Semantic Web. Springer- Verlag, 221–235.

Swartout, B., Ramesh, P., Knight, K. and Russ, T. (1997). Toward Distributed Use of Large- Scale Ontologies. Spring Symposium on Ontological Engineering, 138–148.

Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information and Management, 57 (103334).

Syed, Z., Pädia, A., Finin, T., Mathews, L. and Joshi, A. (2016). UCO: A Unified Cybersecurity Ontology. AAAI Workshop - Technical Report, 195-202.

Takahashi, T. and Kadobayashi, Y. (2011). 3-5 Cybersecurity information exchange techniques: Cybersecurity information ontology and CYBEX. Journal of the National Institute of Information and Communications Technology, 58, 127-135.

Takahashi, T. and Kadobayashi, Y. (2014). Reference Ontology for Cybersecurity Operational Information. Computer Journal, 58, 2297-2312.

Takahashi, T., Kadobayashi, Y. and Fujiwara, H. (2010). Ontological approach toward cybersecurity in cloud computing. 3rd International Conference of Security of Information and Networks, 100109.

Thakur, K. and Pathan, A. (2014). Cybersecurity Fundamentals. CRC Press

Tseng, S., Lin, S., Mao, C., Lee, T., Qiu, G. and Lin, M. (2017). An ontology guiding assessment framework for hacking competition. 10th International Conference on Ubi-Media Computing and Workshops with the 4th International Workshop on Advanced E-Learning and the 1st International Workshop on Multimedia and IoT: Networks, Systems and Applications, 8074131.

Ulanov, A., Shevlyakov, G., Lyubomishchenko, N., Mehra, P. and Polutin, V. (2010). Monte Carlo Study of Taxonomy Evaluation. In Database and Expert Systems Applications (DEXA), 164-168.

Uschold, M. and King, M. (1995). Towards a Methodology for Building Ontologies. Skuce D (eds) IJCAI'95 Workshop on Basic Ontological Issues in Knowledge Sharing, 6.1-6.10.

Van Vuuren, J. J., Leenen, L. and Zaaiman, J. (2014). Using an ontology as a model for the implementation of the national cybersecurity policy framework for South Africa. 9th International Conference on Cyber Warfare and Security 2014, ICCWS 2014, 107-115.

Vega Barbas, M., Villagrá, V. A., Monje, F., Riesco, R., Larriva Novo, X. and Berrocal, J. (2019). Ontology-based system for dynamic risk management in administrative domains.

Wali, A., Chun, S. A. and Geller, J. (2013). A bootstrapping approach for developing a cyber-security ontology using textbook index terms. 2013 International Conference on Availability, Reliability and Security, ARES 2013, 6657291, 569-576.

Welty, C., Mahindru, R. and Chu-Carroll, J. (2003). Evaluating ontological analysis. Semantic Integration Workshop, 92.

Zamfira, A., Fat, R. and Cenan, C. (2019). Applying semantic web technologies to discover an ontology of computer attacks. Scalable Computing, 20, 699-707.

Zamfira, A. C. and Ciocarlie H. (2018). Developing an ontology of cyber-operations in networks of computers. 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing, ICCP 2018, 8516644, 395-400.

Zhao, Y., Lang, B. and Liu, M. (2018). Ontology-based unified model for heterogeneous threat intelligence integration and sharing. International Conference on Anti-Counterfeiting, Security and Identification, ASID, 11-15.

Zheng, H., Wang, Y., Han, C., Le, F., He, R. and Lu, J. (2018). Learning and Applying Ontology for Machine Learning in Cyber Attack Detection. 17th IEEE International Conference on Trust,

Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, 8456049, 13091315.