Informe Técnico / Technical Report

Towards the Consolidation of Cybersecurity Standardized Definitions

Beatriz F. Martins, Lenin J. S.Gil, José F. R. Román, José Ignacio Panach, and Óscar Pastor López

Ref. #:	**PROS-TR-2021-I**
Title:	**Towards the Consolidation of Cybersecurity Standardized Definitions**
Author (s):	**Beatriz Franco. Martins, Lenin Javier Serrano Gil, José Fabián. Reyes. Román, José Ignacio Panach, and Óscar Pastor López**
Corresponding autor (s):	**bmartins@pros.upv.es, lserrano@pros.upv.es, jreyesg@pros.upv.es, joigpana@uv.es, opastor@dsic.upv.es**
Document version number:	**2**
Final version:	**-**
Release date:	**-**
Keywords:	**Conceptualization, Cybersecurity, Knowledge Graphs, Cybersecurity Ontology, Ontology**

Towards the Consolidation of Cybersecurity Standardized Definitions

Beatriz Franco Martins[1 [0000−0001−9190−1047]],

Lenin Javier Serrano Gil[1,2 [0000−0002−1631−7139]],

José Fabián Reyes Román[1 [0000−0002−9598−1301]],

José Ignacio Panach[3 [0000−0002−7043−6227]], and

Oscar Pastor[1 [0000−0002−1320−8471]]

[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

Cybersecurity is a vast and complex domain, therefore enterprises are actively seeking efficient solutions in this matter. Knowledge Graphs (KG) are one of the mechanisms that organizations use to explore the security among assets and possible attacks. However, the great amount of information can create misinterpretation of concepts represented in these structures of conceptualizations. As a KG may be considered an implementation of a conceptualization, the grounding of concepts is fundamental. Therefore, the support of Conceptual Modeling best-practices, especially regarding the branch of Ontologies. We made a pilot study that finds out the state-of-art in "Cybersecurity Ontologies". From this study, we propose a survey to extend our terminological approach. The survey produced a huge amount of data, thus we develop a REST API for data manipulation and a NoSQL database to store them which is the main contribution of this document. Our goal is to provide an ontological analysis tool to help stakeholders avoid misinterpretations during KGs development and implementation.

Keywords: Conceptualization, Cybersecurity, Knowledge Graphs, Cybersecurity Ontology, Ontology

1 Introduction

Nowadays, organizations are focused on the active search for solutions that ensure efficient and safe management and protection of their assets. An application context, especially for large companies, is that of Cybersecurity, which is a broad/extensive and quite complex domain that requires an interdisciplinary approach. One of the mechanisms by which organizations bet to explore security between assets and possible attacks is "Knowledge Graphs" (KG) [59]. Concerning the Conceptual Modeling standpoint, the grounding of concepts is fundamental to implement KG, and it is one of the most relevant ontology applications [17]. That is why the application of ontologies in the cybersecurity domain emerges today as a research topic of great importance and interest. The main objective of this research work is to facilitate a pragmatic and iterative solution that meets the needs of organizations in terms of Cybersecurity, and in this way contribute to Ontology Engineering research.

However, before providing a proposal to achieve this problem, we look for the solution proposals that exist in the state-of-art. Previously, we conducted a pilot study [44] looking for existing works that deal with cybersecurity requirements from an ontological perspective. As the results we took from this research provided a huge amount of data, we develop a Representational State Transfer Application Programming Interface (REST API) for data manipulation and a Not Only SQL (NoSQL) database to store these data. Our goal is to provide data analytics and reasoning using these data and in future work provide a tool to facilitate the process of *Ontological Analyisis* [17]. Through this document, we present the REST API we develop and some initial results these approaches provide.

We have organized the rest of this document in the following way: Section 2 presents the pilot study that supports this work. Section 3 details the proposal of an API to support ontological analysis in complex fields, like cybersecurity. Section 4 depicts the actual state of the proposal with some further research directions.

2 The Pilot Study

There is not a definitive architectural solution for the design and development of KGs supported by ontologies yet. This problem is mainly due to the complexity and interdisciplinarity of the domain. Therefore, we made a pilot study [44] to identify proposals in the cross-field of Cybersecurity and Ontologies, evaluate the existing Cybersecurity Ontologies' level of applicability, and identify the possible data sources of cybersecurity information. In this initial research, we found that the knowledge base for cybersecurity is extensive and context-dependent.

In the pilot study, we support our cybersecurity perspective using the ISO/IEC 27032:2012 [25] and ISO/IEC 27000:2018 [27] standards. These standards make up the knowledge base to identify and detect the most used terms cybersecurity definitions in the presented ontologies in the articles that we found. However, we observe the need to compare the definitions contained in these ontologies with the different definitions in a broad amount of cybersecurity standards. Therefore, we use a NoSQL database to store the standards' definitions and a REST API to analyze them, Secction 3 detail our tool proposal.

From the ISO/IEC standards, we extract 156 terms and their definitions, complying with ontological concepts, and we count the number of its citations in the papers found. To do this, we applied to the articles a semi-automatic technique (a regular expression search cycle) through a sequence of steps.

Automatic Search: We develop a script in Python [4] to obtain the clear text of the documents. Then, we search for terms from the ISO/IEC selected definitions in each

[4] https://docs.python.org/3/reference/

of the documents by executing queries with regular expressions over an algorithm we developed;

Context Validation: We execute another Python algorithm –from the Automatic Keyword Extraction from Individual Documents [57]– to provide context validation. Next, we extract the key phrases using the "RAKE short for Rapid Automatic Keyword Extraction algorithm" implementation do validate. Then, we perform a second round of reading the documents to verify if all terms comply with cybersecurity's context.

Filtering: Lastly, we filter and eliminate the deviation of terms before summarizing the citations from the total of ISO/IEC terms that we got in our sample papers.

This terminological reference base usually presents concepts (or entities) used in ontologies and is mostly supported by all consecrated cybersecurity standards (beyond ISO/IEC used). However, it is out of our scope to guarantee and verify if all terms mean the same conceptual *thing* (in terms of ontological grounding). This semantic adequacy of the conceptualization is future research that is part of the Ontological Engineering process during the course of the project.

Table 1 shows the total number of occurrences of cybersecurity terminology in our pilot study. We use these terms to clarify the semantics of these terms by cross-examining their definitions at the most relevant Cybersecurity standards available. We used the outcomes of our previous pilot study to extract the found terms and use them in our survey, which is also a contribution of this paper.

Table 1. Cybersecurity perspective – total of citations according to ISO/IEC 27000 and ISO/IEC 27032 terminology from the pilot study [44].

Term	Total of citations
Access Control	30
Application	208
Asset	348
Attack	942
Authentication	14
Bot	121
Availability	61
Competence	2
Confidentiality	37
Consequence	61
Control	154
Countermeasure	75
Event	333
Indicator	9

Term	Total of citations
Information Need	5
Information Security	40
Information System	8
Integrity	45
Internet	96
Likelihood	14
Malicious Software	3
Malware	218
Measure	117
Measurement	6
Monitoring	82
Objective	29
Organization	271
Performance	33
Phishing	3

Term	Total of citations
Policy	117
Process	401
Provider	75
Reliability	11
Requirement	93
Review	42
Risk	259
Risk Assessment	10
Risk Management	7
Stakeholder	50
Threat	348
Trojan	12
Trojan Horse	2
Vulnerability	775

3 Terminological Investigation

Next we describe the details of the terminological investigation we conduct.

3.1 Objective

Our main goal is to identify the existence of definitions for the terms contained in the ISO/IEC 27032:2012 and ISO/IEC 27000:2018 standards in a broad set of other documents accepted by cybersecurity community. These terms are present in the primary studies that describe the design and implementation of ontologies for the domain of Cybersecurity. Therefore, we expect to consolidate the definitions of each term and identify the context of the use of them based on the standards they belong to. Lastly, we can identify possible misinterpretations on cybersecurity ontologies concerning the terminology used by them.

In summary, our goal is **to identify and evaluate the existing Cybersecurity Ontologies' terminology, their context, and use**.

3.2 Cybersecurity Standards

Definitions used by standards such as those in ISO/IEC exist to clarify the interpretation of terms present in the knowledge domain of those standards. 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. Therefore, we expand our cybersecurity perspective, providing a terminological investigation based on the verification we made at the pilot study. We use the terms previously found at the studies' verification to look for definitions of these terms in additional recognized standards by the cybersecurity community. Table 2 shows the standards we use.

Table 2. Cybersecurity perspective – validation standards besides ISO/IEC 27032:2012 [25] and ISO/IEC 27000:2018 [27].

Institution	Standard
ISO and IEC	ISO/IEC 154081:2009 [24], ISO/IEC 154082:2008 [22], ISO/IEC 154083:2008 [23], ISO/IEC ISO/IEC 27002:2013 [26]
ITU-T	ITU-T-RecX805 [35], ITU-T-RecX810 [30], ITU-T-RecX811 [32] ITU-T-RecX812 [33], ITU-T-RecX813 [34], ITU-T-RecX814 [29], ITU-T-RecX815 [28], ITU-T-RecX816 [31], RecITU-T-X1205 [36], RecITU-T-X1209 [37], RecITU-T-X1212 [39], RecITU-T-X1500 [38]
CCITT & ITU-T	Data Communication Networks: Open Systems Interconnection (OSI) [7]
CCMB	CCDB-2017-05-xxx [6], CCMB-2017-04-001 [8], CCMB-2017-04-002 [9], CCMB-2017-04-003 [10], CCMB-2017-04-004 [11]
NIST	Framework for Improving Critical Infrastructure Cybersecurity (NIST-CSWP-04162018) [48], Framework for Improving Critical Infrastructure Cybersecurity (NIST-CSWP-04162014) [47], Security Self-Assessment Guide for Information Technology Systems [46], Digital Identity Guidelines [1], Digital Identity Guidelines: Enrollment and Identity Proofing [14], Digital Identity Guidelines: Authentication and Lifecycle Management [15], An Introduction to Information Security An Introduction to Information Security [52], Guide to ICS Security NIST Special Publication 800-82 [62], Risk Management Framework for Information Systems and Organizations [40], Generally accepted principles and practices for securing information technology systems [53], Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations [41], National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [51], Federation and Assertions [60]
MAEC 50	MAEC™ Specification - Core Concepts [42], MAEC™ Specification - Vocabularies [43]
OASIS Committee Specification	STIX™ Version 2.1 [5], TAXII™ Version 2.1 [64]
MITRE Corporation	CVE-1999-0001 [4], MITRE ATT & CK: Design and Philosophy [63], Ten Strategies of a World-Class Cybersecurity Operations Center [65], Science of Cyber-Security [45], Standardizing Cyber Threat Intelligence Information with the STIX™ [2] The trusted automated exchange of indicator information (TAXII™) [13]
NERC	Glossary of Terms Used in NERC Reliability Standards [50] CIPC Control Systems Security Working Group (NERC-CIPv3-v5) [49]
CCRA	Common Criteria Portal (CCv31-Release 5) [12]
Spain Government	Security Guide (CCN-STIC-401) [16]
Spanish National Cybersecurity Institute	Cybersecurity Terms Glossary [21]
Common Criteria	Standard 1300 - Cyber Security [61]

3.3 Consolidating Definitions

To consolidate the definitions of the terms previously found in the studies, we propose a survey because the amount of standards is vast as well as the number of terms. We invite 18 (eighteen) cybersecurity students to participate in this survey [58]. It is important to note that the survey is part of a collaboration with the Department of Systems Engineering and Informatics of the Universidad Pontificia Bolivariana (UPB, Colombia) [5].

The students searched for each term one or more definitions in all these standards. We define a questionnaire with a spreadsheet template in which the students present their impressions about the meaning, context, and use of each definition depending on which source it is. We divided the terms among the students, so each student worked with only two different terms, summing a total of 36 terms. However, the students were able to add additional terminology that composes a set of regular expressions with these terms. Therefore, we cover 43 of the terms found in the papers pilot study search. The students had two weeks to present their results.

Meanwhile, we developed a NoSQL database[6] and the REST API [7] to store and manipulate the resulting survey data. Then, we consolidate all standards (sources), terms, and definitions of the survey through the API developed. Below we present an API code fragment responsible to query definitions by regular expressions (RegEx).

```
...
// Get definitions list by regex
function getDefinitionsByRegEx(req,res){
    var definition = new Definition();
    definition.regex = req.params.regex;

    Definition.aggregate([
        { $match: { regex : definition.regex } },
        { $lookup: {
            from: "sources",
            localField: "source",
            foreignField: "_id",
            as: "source" }
        }
        ]).exec((err,definitions) => {
        if(err) return res.status(500).send({message: 'Incorrect
             request.'});

        return res.status(200).send({definitions});
    });
}
...
```

We can see one example of the results produced through this code with the term *Confidentiality* that has several definitions. The code below shows a fragment of this

[5] https://www.upb.edu.co/es/home
[6] Stored thought a MongoDB (https://www.mongodb.com/) database
[7] Implemented with NodeJS (https://nodejs.org/en/)

term's querying result [8] took (http://localhost:3800/api/definitionsByRegEx/) over our database.


```json
{
    "definitions": [
        {
            "source": [
                {
                    "label": "CCMB-2017-04-002",
                    "file": "J4OW9SX8G3wTZHa7jY_AE5MZ.pdf"
                }
            ],
            "text": "Confidentiality is enforced by preventing unauthorised disclosure of user data in transit between the two end
                    points.\nThe end points may be a TSF or a user. Confidentiality of TSF Data during transmission is necessary to
                    protect such\ninformation from disclosure. Some possible implementations that could provide confidentiality
                    include the use of cryptographic algorithms as well as spread spectrum techniques.",
            "locale": "F.12, 907"
        },
        {
            "source": [
                {
                    "label": "CCMB-2017-04-004",
                    "file": "C52E9zeyWY9A4mKyYupe19r_.pdf"
                }
            ],
            "text": "An evaluator may have access to sponsor and developer commercially-sensitive information (e.g. TOE design
                    information, specialist tools), and may have access to nationally-sensitive information during the course of an
                    evaluation. Schemes may wish to impose requirements for the evaluator to maintain the confidentiality of the
                    evaluation evidence. The sponsor and evaluator may mutually agree to additional requirements as long as these
                    are consistent with the scheme.\nConfidentiality requirements affect many aspects of evaluation work, including
                    the receipt, handling, storage and disposal of evaluation evidence.",
            "locale": "8.3.3.3, 70and 71"
        },
        {
            "source": [
                {
                    "label": "CCv31-Release 5",
                    "url": "https://www.commoncriteriaportal.org/cc/",
                    "file": "Ire3UpmtCzQvwRGzEj5uM-CG.xml"
                }
            ],
            "text": "An evaluator may have access to sponsor and developer commercially-sensitive information (e.g. TOE design
                    information, specialist tools), and may have access to nationally-sensitive information during the course of an
                    evaluation. Schemes may wish to impose requirements for the evaluator to maintain the confidentiality of the
                    evaluation evidence. The sponsor and evaluator may mutually agree to additional requirements as long as these
                    are consistent with the scheme.\nConfidentiality requirements affect many aspects of evaluation work, including
                    the receipt, handling, storage and disposal of evaluation evidence.",
            "locale": "line 6476,<subclause title=\"Confidentiality\"
                    id=\"general-evaluation-tasks-evaluation-input-task-confidentiality\"> "
        },
        {
            "source": [
                {
                    "label": "ISOIEC270002018",
                    "file": "lImYLf8G2vUt6oLx7qB2Tnzh.pdf"
                }
            ],
            "text": "confidentiality\nproperty that information is not made available or disclosed to unauthorized individuals,
                    entities, or processes (3.54)",
            "locale": "3.10"
        },
        {
            "source": [
                {
                    "label": "RecX800",
                    "file": "wOOhiraYzBq2_5kqBF_NbyBB.pdf"
                }
            ],
            "text": "The property that information is not made available or disclosed to unauthorized individuals, entities,
                    or\nprocesses.",
            "locale": "3.3.16"
        },
        {
            "source": [
                {
                    "label": "RecITU-T-X1212",
                    "file": "XjDGxE28rZybwMDywwpMMchn.pdf"
                }
```


[8] The JSON file was edited suppressing, the surplus of data. The objective is to provide a better presentation and reduce size.

```
60          ],
61          "text": "Three enabling concepts of information security\nConfidentiality\nMeasured data may include personal
                   information, which is essentially privacy sensitive. Thus, the use of such data needs to be handled carefully,
                   accompanied by agreement with end users. The extent of sharing such information must be under strict control.",
62          "locale": "1.2"
63      },
64      {
65          "source": [
66              {
67                  "label": "Nieles",
68                  "file": "UtpHAsXfNjG9ahRwteN7HuQV.pdf"
69              }
70          ],
71          "text": "Confidentiality - Preserving authorized restrictions on information access and disclosure, including means
                   for protecting personal privacy and proprietary information.",
72          "locale": "1.4"
73      },
74      {
75          "source": [
76              {
77                  "label": "NIST800-37Revision2",
78                  "file": "7BoFnjKwNtPgcgkbKGjEmSVp.pdf"
79              }
80          ],
81          "text": "confidentiality\n[44 USC 3552]\nPreserving authorized restrictions on information access and disclosure,
                   including means for protecting personal privacy and proprietary information.",
82          "locale": "Appendix B, pag 93"
83      },
84      {
85          "source": [
86              {
87                  "label": "NIST800-53Rev4",
88                  "file": "e6QRCYw4txC43AJgw5-LJFie.pdf"
89              }
90          ],
91          "text": "Confidentiality\n[44 U.S.C., Sec. 3542]\nPreserving authorized restrictions on information access and
                   disclosure, including means for protecting personal privacy and proprietary information.",
92          "locale": "Appendix B, pag B-5"
93      },
94      {
95          "source": [
96              {
97                  "label": "Stouffer",
98                  "file": "Yjqu3eLKaRTO9Bf-PXaRbGNX.pdf"
99              }
100         ],
101         "text": "Confidentiality\nPreserving authorized restrictions on information access and disclosure, including means for
                   protecting personal privacy and proprietary information.\nSOURCE: NIST SP 800-53 [22]",
102         "locale": "Appendix B, pag B2"
103     },
104     {
105         "source": [
106             {
107                 "label": "SpecPubl800-26",
108                 "file": "UO77OeEpdg-GJRRsIdVcRxtr.pdf"
109             }
110         ],
111         "text": "Confidentiality - The information requires protection from unauthorized disclosure.",
112         "locale": "2.2, pag 5"
113     }
114   ]
115 }
```

Firstly, the very same definitions appear in different sources: line 31 [12] is the same as 20 [11], line 51 [7] is the same as 41 [27], and lines 81 [40], 91 [41] and 101 [62] are same as 71 [52]. However only one of those is the primary source while the others are references to it, in this case, the primary sources are at the lines, respectively the 31 [12] in the previous release, 51 [7], and 91 [41]. With this tool we intend to gather all the considering domain terminology definitions according to their sources, to facilitate our analysis.

In common, all definitions consider the term `Confidentiality` a **Property** that can be assigned to many different **Individuals**[9]. Some of the aforementioned refer to

[9] Property and Individuals in the ontological sense [18]

kinds of *Information* like *Proprietary*, *Sensitive* or *Personal*, others refers to *User Data*. Indeed it is important to see that the *Data* term's meaning is not the same as *Information* since not all data refers to information. Moreover, in a step forward we need to determine if the property of some individual being `Confidential` is quantified or not; and if it is, what is its quality structure the and how to measure if (it is possible) [20]. This kind of analysis is an example of how terminological validation is important, indeed this is part of an ontological analysis concerning the cybersecurity domain.

Another example of the use of the API refers to the ontologies we found. In this case, we intend to cross the ontology analysis results, including the definitions it uses, with the standards' definitions. The code below shows a fragment of the information we collect about the SECCO ontology, which is a sub-ontology of CRATELO [55,56,54,3].

```
...
// Get ontology
function getOntology(req,res){
    var ontology = new Ontology();
    ontology._id = req.params.id;

    Ontology.aggregate([
        { $match: { _id : ontology._id } },
        { $lookup : {
            from : "definitions",
            localField : "definitions",
            foreignField : "_id",
            as : "definitions" }
        },
        { $lookup: {
            from: "regexes",
            localField: "definitions.regex",
            foreignField: "_id",
            as: "regex" }
        },
        { $lookup : {
            from : "terms",
            localField : "regex.term",
            foreignField : "_id",
            as : "term" }
        },
        { $graphLookup : {
            from : "regexes",
            startWith : "$regex.next",
            connectFromField : "regex.next",
            connectToField : "_id",
            as : "next" }
        },
        { $lookup: {
            from: "ontologies",
            localField: "subOntologyOf",
            foreignField: "_id",
```

```
            as: "subOntologyOf" }
        },
        { $lookup: {
            from: "ontologies",
            localField: "groundedOver",
            foreignField: "_id",
            as: "groundedOver" }
        },
        { $lookup: {
            from: "ontologies",
            localField: "implementationFor",
            foreignField: "_id",
            as: "implementationFor" }
        }
    ]).exec((err,ontology) => {
        if(err) return res.status(500).send({message: 'Incorrect
            request.'});

        if(!ontology) return res.status(404).send({message: 'Unknow
            ontological analysis.'});

        return res.status(200).send({ontology});
    });
}
...
```

This code result presents the information we catch about the SECCO ontology, as below (http://localhost:3800/api/ontology/). We can see that the result also shows the definitions this ontology use and from which source these definitions came. The source can be any standard or document. Here we reduce file results showing only one definition since the file is large.


```
{
    "ontology": [
        {
            "_id": "600f1eaa10370e2e78c743d8",
            "definitions": [
            ...
                {
                    "_id": "600f5a13d289480c60440184",
                    "source": "600f59aed289480c60440183",
                    "regex": "5eee523ad541e23b1e3855cb",
                    "text": "(Risk). The risk is the probability that a successful attack occurs.",
                    "locale": "pag 94"
            },
            ...
            ],
            "cqs": [],
            "name": "SECCO",
            "domain": "Security",
            "subOntologyOf": [
                {
                    "_id": "600d7f5af2b31f1bb0080d7c",
                    "definitions": [],
                    "cqs": [],
                    "name": "CRATELO",
                    "domain": "Cybersecurity",
                    "language": "OWL-Lite"
                }
            ],
            "language": "OWL-Lite",
```

```
            "groundedOver": [
                {
                    "_id": "601ae4a800271e2caca0245f",
                    "definitions": [],
                    "cqs": [],
                    "name": "DOLCE-Spray",
                    "domain": "General",
                    "language": "OWL-Lite",
                    "implementationFor": "601ae1769bbf9122c8a732cf"
                }
            ],
            "regex": [
            ...
                {
                    "_id": "5eee523ad541e23b1e3855cb",
                    "term": "5eee4e7a6df9e92524876507"
            },
            ...
            ],
            "term": [
            ...
                {
                    "_id": "5eee4e7a6df9e92524876507",
                    "syntax": "risk"
            },
            ...
            ],
            "next": [],
            "implementationFor": []
        }
    ]
}
```


All of this denotes how huge and complex is to provide a conceptualization of the cybersecurity domain. Therefore, one of the goals of the survey we made and its resulting API is to get together domain terminology definitions according to their sources, to facilitate our analysis. Then, we are cross comparing the result of this analysis with the definitions used in the ontologies we found in the pilot study, as a next step.

4 Conclusions

In this document, we present our proposal for an API in which we can consolidate definitions of the terms used in the cybersecurity domain. We present an example showing how complex is the set of definitions for a single concept, indeed this complexity gets increased concerning the vast amount of concepts, their relations, and the context in which they are applied. Our intention is also to analyze the standard support that provides the grounding for the concepts over the cybersecurity domain.

The API using a NoSQL database sounds a relevant contribution to help Ontology Engineers on ontological analysis where complex domains are the scenario. The objective of this kind of approach is to identify the semantics of the concepts used, their similarities, and differences. From this initial step, we aim to provide a link between the domain terminology, its context with its representations in ontologies, following the approach of [19]. Besides, the control of this information allows us to do reasoning and present results from a friendly interface, both are future research works preceding a final solution proposal to provide interoperability among ontologies implemented as KGs.

Acknowledgments. This work has been developed under the project Digital Knowledge Graph – Adaptable Analytics API with the financial support of Accenture LTD.

References

1. And, P.A.G., And, M.E.G., Fenton, J.L.: Digital Identity Guidelines. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-63-3
2. Barnum, S.: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX ™). Mitre Corporation **11**(Version 1.1, Revision 1), 1–22 (2014)
3. Ben-Asher, N., Oltramari, A., Erbacher, R.F., Gonzalez, C.: Ontology-based adaptive systems of cyber defense. In: STIDS. pp. 34–41 (2015)
4. Board, C.E.: Common Vulnerabilities and Exposures - CVE downloads data last generated: 2020-06-23. https://cve.mitre.org/data/downloads/index.html (2006), [Online; accessed 23-Jun-2020]
5. Bret Jordan, Rich Piazza, and Trey Darley (ed.): OASIS - STIX™ Version 2.1. OASIS Committee Specification 01 (2020)
6. CCDB (ed.): CC and CEM addenda Exact Conformance , Selection-Based SFRs , Optional SFRs, vol. V0.5. CCDB, Geneva - Switzerland (May 2017)
7. CCITT & ITU-T (ed.): DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATION - SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS. CCITT & ITU-T, Geneva - Switzerland (1991)
8. CCMB (ed.): Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model, vol. Version3.1. CCDB, revision 5 edn. (2017)
9. CCMB (ed.): Common Criteria for Information Technology Security Evaluation Part 2 : Security functional components, vol. Version3.1. CCDB, revision 5 edn. (2017)
10. CCMB (ed.): Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components, vol. Version3.1. CCDB, revision 5 edn. (2017)
11. CCMB (ed.): Common Methodology for Information Technology Security Evaluation Evaluation methodology, vol. Version3.1. CCDB, revision 5 edn. (2017)
12. CCRA: Common Criteria Portal. https://www.commoncriteriaportal.org/cc/ (2017), [Online; accessed 23-Jun-2020]
13. Connolly, J., Davidson, M., Schmidt, C.: The trusted automated exchange of indicator information (taxii). The MITRE Corporation pp. 1–20 (2014)
14. Fenton, J.L., Lefkovitz, N.B., Danker, J.M., Greene, K.K., Theofanos, M.F.: Digital Identity Guidelines: Enrollment and Identity Proofing. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-63a
15. Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E., Richer, J.P., Lefkovitz, N.B., Danker, J.M., Greene, K.K., Theofanos, M.F., Newton, E.M., Burr, W.E.: Digital Identity Guidelines: Authentication and Lifecycle Management. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-63b
16. GUÍA DE SEGURIDAD (CCN-STIC-401) GLOSARIO Y ABREVIATURAS (2015)
17. Guarino, N.: Formal Ontology in Information Systems. In: Proceedings of the 1st International Conference. pp. 6–8. IOS Press, Trento, Italy (June 1998)
18. Guarino, N.: The ontological level. Philosophy and the Cognitive Sciences (1994)
19. Guarino, N.: The ontological level: Revisiting 30 years of knowledge representation. Conceptual modeling: Foundations and applications pp. 52–67 (2009)
20. Guizzardi, G., Zamborlini, V.: Using a trope-based foundational ontology for bridging different areas of concern in ontology-driven conceptual modeling. Science of Computer Programming **96**, 417–443 (2014)
21. Instituto Nacional de Ciberseguridad - Spanish National Cybersecurity Institute (ed.): Glosario de términos de ciberseguridad - Una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad - Spanish National Cybersecurity Institute (2017)

22. ISO Central Secretary: Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components. Standard ISO/IEC 154082:2008, International Organization for Standardization, Geneva (2008)
23. ISO Central Secretary: Information technology Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components. Standard ISO/IEC 154083:2008, International Organization for Standardization, Geneva (2008)
24. ISO Central Secretary: Irmation technology — Security techniques — Evaluation criteria for IT — Part 1: Introduction and general model Technologies. Standard ISO/IEC 154081:2009, International Organization for Standardization, Geneva (2009)
25. ISO Central Secretary: Information technology — security techniques — guidelines for cybersecurity. Standard ISO/IEC 27032:2012, International Organization for Standardization, Geneva (2012)
26. ISO Central Secretary: Information technology — Security techniques — Code of practice for information security controls. Standard ISO/IEC 27002:2013, International Organization for Standardization, Geneva (2013)
27. ISO Central Secretary: Information technology — security techniques — information security management systems — overview and vocabulary. Standard ISO/IEC 27000:2018-02, International Organization for Standardization, Geneva (2018)
28. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATION SECURITY - INFORMATION TECHNOLOGY - OPEN SSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS: INTEGRITY FRAMEWORKS, vol. 11/95. ITU-T, Geneva - Switzerland (1995)
29. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS - SECURITY - INFORMATION TECHONOLOGY - OPEN SYSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS: CONFIDENTIALITY FRAMEWORK, vol. 11/95. ITU-T, Geneva - Switzerland (1995)
30. ITU-T (ed.): Data Networks and Open System Communications - Security - Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Overview, vol. 11/95. ITU-T (1996)
31. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS - SECURITY - INFORMATION TECHNOLOGY - OPEN SYSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS: SECURITY AUDIT AND ALARMS FRAMEWORK, vol. 11/95. ITU-T, Geneva - Switzerland (1996)
32. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS - SECURITY - INFORMATION TECHONOLOGY - OPEN SYSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS: AUTHENTICATION FRAMEWORK, vol. 04/95. ITU-T, Geneva - Switzerland (1996)
33. ITU-T (ed.): DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS SECURITY - INFORMATION TECHNOLOGY - OPEN SYSTEMS INTERCONNECTION - SECURITY FRAMEWORKS FOR OPEN SYSTEMS : ACCESS CONTROL, vol. 11/95. ITU-T, Geneva - Switzerland (1996)
34. ITU-T (ed.): SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATION - Security - Information techology - Open Systems Interconnection - Security Frameworks in open systems: Non-repudiation framework, vol. 10/96. ITU-T (1997)
35. ITU-T (ed.): SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS Security - Security architecture for systems providing end-to-end communications, vol. 10/2003. ITU-T (2003)
36. ITU-T (ed.): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security - Overview of cybersecurity, vol. 04/2008. ITU-T (2008)

37. ITU-T (ed.): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Cyberspace security – Cybersecurity - Capabilities and their context scenarios for cybersecurity information sharing and exchange, vol. 12/2010. ITU-T, 1.0 edn. (2010)
38. ITU-T (ed.): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY- Cybersecurity information exchange – Overview of cybersecurity - Overview of cybersecurity information exchange, vol. 04/2011. ITU-T, 1.0 edn. (2012)
39. ITU-T (ed.): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Cyberspace security – Cybersecurity - Design considerations for improved end-user perception of trustworthiness indicators, vol. 03/2017. ITU-T, 1.0 edn. (2017)
40. JOINT TASK FORCE: Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy. Tech. rep., NIST (2018). https://doi.org/https://doi.org/10.6028/NIST.SP.800-37r2
41. JOINT TASK FORCE TRANSFORMATION INITIATIVE: Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations. Tech. rep., NIST (2013). https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-53r4
42. MAEC™ Specification - Core Concepts (2017)
43. MAEC™ Specification - Vocabularies (2017)
44. Martins, B.F., Serrano, L., Reyes, J.F., Panach, J.I., Pastor, O., Rochwerger, B.: Conceptual characterization of cybersecurity ontologies. In: 13th IFIP WG 8.1 working conference on the Practice of Enterprise Modelling (PoEM 2020). pp. 323–338. Springer (2020)
45. Mitre Corporation: Science of Cyber-Security. Tech. rep., The MITRE Corporation, McLean, Virginia (2010)
46. National Institute of Standards and Technology: Security Self-Assessment Guide for Information Technology Systems. Tech. rep., National Institute of Standards and Technology, Gaithersburg, MD (2001)
47. National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity. Tech. rep., National Institute of Standards and Technology (2014)
48. National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity. Tech. rep., National Institute of Standards and Technology (2018). https://doi.org/https://doi.org/10.6028/NIST.CSWP.04162018
49. NERC: CIPC Control Systems Security Working Group. Tech. rep., NERC (2014)
50. NERC: Glossary of Terms Used in NERC Reliability Standards. Tech. rep., NERC (2020)
51. Newhouse, W., Newhouse, W., Scribner, B., Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-181
52. Nieles, M., Dempsey, K., Pillitteri, V.Y.: An Introduction to Information Security An Introduction to Information Security. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-12r1
53. NIST (ed.): Generally accepted principles and practices for securing information technology systems. NIST (2018)
54. 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)
55. Oltramari, A., Cranor, L.F., Walls, R.J., McDaniel, P.D.: Building an ontology of cyber security. In: STIDS. pp. 54–61. Citeseer (2014)
56. Oltramari, A., Henshel, D.S., Cains, M., Hoffman, B.: Towards a human factors ontology for cyber security. In: STIDS. pp. 26–33 (2015)

57. 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)
58. Serrano, L., Martins, B.F., Serrano, J.F., Panach, J.I., Pastor, O.: Una encuesta acerca de la Definición de Conceptos de Ciberseguridad. Tech. rep., Universidad Politecnica de Valencia (2021)
59. Singhal, A., Ou, X.: Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs, pp. 53–73. Springer International Publishing (2017)
60. Squire, S.K., Fenton, J.L., Nadeau, E.M., Danker, J.M., Greene, K.K., Theofanos, M.F.: Federation and Assertions. Tech. rep., NIST (2017). https://doi.org/https://doi.org/10.6028/NIST.SP.800-63c
61. Standard 1300 — Cyber Security (2004)
62. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A.: Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control Syst. Tech. rep., NIST (2015). https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-82r2
63. Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B.: MITRE ATT&CK(trademark): Design and Philosophy. Tech. rep., The MITRE Corporation, McLean, VA (2018 (revised 2020))
64. Varner, B.J., Drew (eds.): OASIS - TAXII™ Version 2.1. OASIS Committee Specification 01 (2020)
65. Zimmerman, C.: Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation, Bedford, MA (2014)