

SECURITY ONTOLOGY IN A VIRTUAL UNIVERSITY

Loredana MOCEAN

Babeş-Bolyai University, Cluj-Napoca, Romania
loredana.mocean@ubbcluj.ro

Miranda-Petronella VLAD

“Dimitrie Cantemir” Christian University, Bucharest, Romania
miranda.vlad@cantemircluj.ro

ABSTRACT

In this paper we propose a cybersecurity ontology model designed for universities, aiming to facilitate the management and protection of sensitive data and information within the context of the growing cybersecurity threats. The proposed ontology includes four distinct hierarchical levels: the basic level, the conceptual level, the instance level and the relationships level. At the basic level, it defines essential terms and principles of cybersecurity, including concepts like vulnerability, threat, cyber-attack, security policies and security rules. At the conceptual level, the ontology categorizes information and cybersecurity systems, embracing domains such as data protection, authentication, authorization, and auditing. At the instance level, the ontology describes specific examples of information and cybersecurity systems used in universities, such as the library management system or the accounting management system. At the relationships level, the ontology establishes links between different categories of information and cybersecurity systems, as well as between these systems and the entities that use them, such as students, professors and administrative staff. By implementing this cybersecurity ontology, universities can improve the management and protection of their sensitive data and information, as well as respond more efficiently to cybersecurity threats.

KEYWORDS: cybersecurity, ontology, university, instance, classes

1. Introduction

Technological progress has transformed not only the business sector, but also the educational and academic sectors. Over the past few years, higher education institutions have registered a rapid growth, primarily attributed to the adoption of advanced technologies, state Gligorea et al. (2022).

In this context, Dinicu et al. (2021) in their study paper highlight the impact on different facets of the global social system that can grow from a critical infrastructure malfunctioning due to a cyberattack.

Threats and vulnerabilities can also be prevented using security ontologies. In the field of computer security, there are several

security ontologies that are used to describe and classify different types of threats and vulnerabilities.

Ontology is a formal knowledge representation structure that uses a hierarchical classification scheme to organize information in a coherent and easily understandable manner.

There are some important papers that present an overview of ontologies in Information Systems Security. Several works targeting different aspects of security engineering are presented together with studies that compare several publicly available security ontologies, as say Gomes et al. (2001).

Borja Rivadeneira & Gómez (2020) report the findings of a systematic review of the literature on ontologies in the field of cybersecurity. Within this study, the authors answered research questions related to the domains in which ontologies are used, the methodologies, tools and languages used, and the verification and validation mechanisms reported.

Here are some examples of security ontologies:

1. *Common Vulnerability Scoring System* (CVSS), a security ontology used to evaluate the severity of vulnerabilities in computer systems. (<https://www.techtarget.com/searchsecurity/definition/CVSS-Common-Vulnerability-Scoring-System>).

2. *Common Attack Pattern Enumeration and Classification* (CAPEC), a security ontology used to classify types of cyber-attacks (<https://capec.mitre.org/>).

3. *Open Web Application Security Project* (OWASP) serves as a security ontology applied to the detection and mitigation of vulnerabilities within web applications (<https://info.opswat.com/dm/>).

4. *Structured Threat Information eXpression* (STIX) functions as a security ontology utilized to present information concerning cyber threats in a uniform and standardized manner (<https://www.techtarget.com/searchsecurity/definition/STIX-Structured-Threat-Information-eXpression>).

5. *Cyber Observable eXpression* (CybOX) is a security ontology utilized to represent data pertaining to security events and entities in a standardized format (<https://cyware.com/security-guides/cyber-threat-intelligence/what-is-cybox-how-do-you-use-a-cybox-object-af90>).

These ontologies are used to enhance interoperability and collaboration among various cyber security solutions and tools.

2. A Brief Comparison between Security Ontologies

The security ontologies presented above, have distinctive attributes and

characteristics and are frequently used in conjunction to fulfill particular security objectives. Below are some comparative aspects among these security ontologies:

1. **Purpose:** Each security ontology serves a defined purpose. For instance CVSS is employed to assess the severity of vulnerabilities and CAPEC is employed to categorize various cyber-attack types. On the other hand, STIX and CybOX function as security ontologies for the standardized representation of cyber threat information and security entities.

2. **Structure:** The structure of security ontologies may differ, but most include a set of classes or terms to systematically organize information. For instance, CVSS uses its database to evaluate vulnerabilities based on their severity. In contrast, OWASP consists of a series of projects that address various facets of security.

3. **Focus:** CVSS concentrates on assessing vulnerability severity, while CAPEC centers on classifying cyber-attack types. OWASP's focus is on identifying vulnerabilities in web applications, while STIX and CybOX concentrate on the standardized representation of cyber threat information.

4. **User Orientation:** CVSS, CAPEC, and OWASP are designed with a user-oriented approach, serving security administrators, auditors, and other cybersecurity specialists. STIX and CybOX adopt a more machine-oriented approach, catering to automated cybersecurity tools for the standardized representation of cyber-threat information.

5. **Duration of Service:** CVSS, CAPEC, and OWASP are well-established and have been in use for a longer period, enjoying greater recognition. STIX and CybOX, on the other hand, are newer and less spread but are gaining popularity.

In conclusion, each security ontology has a set of distinct characteristics and specific utility in particular cybersecurity contexts.

3. Models of Cybersecurity

Several cybersecurity models are available for protecting computer systems and networks against cyberattacks. Here are some examples of these cybersecurity models:

1. *The AAA Model* – Authentication, Authorization, and Accounting, is a cybersecurity model designed to protect computer networks and systems. It ensures authentication, authorization, and tracks user activity (Source: [TechTarget](#)).

2. *The Defense-in-Depth Model*. This model implements multiple layers of protection to defend computer systems and networks against cyberattacks (Source: [CISecurity](#)).

3. *The NIST Cybersecurity Framework* was developed by the National Institute of Standards and Technology (NIST) and offers a comprehensive approach to managing cyber risks (Source: [NIST](#)).

4. *The CIA Model* – Confidentiality, Integrity, and Availability. This model is a well-established cybersecurity model. It emphasizes safeguarding information by ensuring its confidentiality, integrity, and availability (Source: [TechTarget](#)).

5. *The Zero Trust Model*. This is a modern and new cybersecurity model and has a basic principle that no entity, whether a person or system, can be presumed trusted. Continuous verification is required for access to sensitive resources (Source: [NordLayer](#)).

These models present systematic methodologies for enhancing the security of computer systems and networks against cyber threats.

Each model has its distinct advantages and limitations, and the selection of a specific model depends on the particular requirements of an organization and its computer infrastructure. Numerous universities have adopted ontology models in the realm of cybersecurity, and here are some examples:

1. *University of New South Wales (UNSW)*: UNSW's Cyber Security Ontology Model uses natural language-based ontologies to represent concepts and relationships between cyber threats, vulnerabilities and defenses. This model was effective in vulnerability detection and security analysis.

2. *Carnegie Mellon University*: Carnegie Mellon's cybersecurity ontology model, known as CybOX (Cyber Observable eXpression) provides a standardized ontology for representing cyber threat information. It includes standardized terms for describing common data types like IP addresses, files, and processes.

3. *University of Maryland* has developed the CAE (Cybersecurity Analysis and Experimentation) ontology model. It serves as a basic ontology for representing cybersecurity concepts and their relationships. It has been instrumental in building a cybersecurity analysis framework for evaluating and enhancing cybersecurity systems.

These examples show how universities use ontology models to improve cybersecurity. Numerous other university models are actively involved in developing such frameworks to improve cybersecurity practices.

4. Ontology Model for Cybersecurity

The ontology model of cybersecurity typically includes a set of classes, properties, and axioms that describe the different entities in the domain, such as threats, vulnerabilities, assets and controls.

It also includes a set of rules that define how these entities relate to each other, as well as to different types of attacks, defense strategies and risk management approaches.

The classes can possibly be (see Table no. 1):

Table no. 1*Classes for a cybersecurity model*

Class	Subclass	Services
“Threats”	<i>types of threats</i>	virus attacks, denial-of-service attacks, phishing, spoofing, etc.
“Vulnerabilities”	<i>types of vulnerabilities</i>	network vulnerabilities, system vulnerabilities, application vulnerabilities, etc.
“Security Policies”	<i>types of security policies</i>	authentication policies, authorization policies, auditing policies.
“Security Measures”	<i>types of security measures</i>	firewalls, intrusion detection systems, antivirus.
“Security Incidents”	<i>types of security incidents</i>	unauthorized access to a computer system, malware infection on a computer/network, social engineering attacks, phishing, pretexting, denial-of-service attacks.

This ontology model for cybersecurity can be used to manage cybersecurity-related information and resources in a structured and coherent way. It can also be adapted to fit the specific

needs of an organization or an information system. Here is a possible ontology model for cybersecurity in a university (as we see in Table no. 2):

Table no. 2*Ontology model for cybersecurity in a university*

Class	Subclass	Services
“Educational Activities”	<i>types of courses, seminars, lectures</i>	dates of the activity, the number of participants, and information about the platform used.
“Data and Information”	<i>types of data and information</i>	network vulnerabilities, system vulnerabilities, application vulnerabilities.
“Threats”	<i>types of cyber-attacks, phishing, hacking</i>	threat's characteristics, how it works, solutions of protection.
“Vulnerabilities”	<i>types of network vulnerabilities, system vulnerabilities and application vulnerabilities</i>	vulnerability's characteristics, ways to detect and prevent it.
“Security Incidents”	<i>types of security incidents, cyber-attacks, data loss</i>	information about the incident's characteristics, detection and reports, information about the measures taken to remediate the situation.
“Security Measures”	<i>firewalls, intrusion detection systems, antivirus</i>	security measure's characteristics, how it works, ways of implementation and monitoring.
“Security Policy”	<i>security incidents</i>	cyber-attacks, data loss, authentication, auditing.

5. The Proposed Model

The framework described in the paper of Georgescu & Smeureanu (2017), can be a point of start in the improvement of cybersecurity by means of semantic web technologies.

There are numerous ontology-based methods in the cybersecurity field which have been created with the objective of addressing the challenge of detecting vulnerabilities in actual systems (Pastuszuk, Księżopolski & Burek, 2021).

Léger, Gagnon & Valverde (2021) described an ontology engineering methodology for cybersecurity while De Rosa et al. (2021) and Modiba, Ojo & Ncube (2019) described engineering methodologies for ontologies.

As we know, ontology can be defined as a formal structure of knowledge that describes and organizes the relationships between different types of entities or concepts.

In the context of a university, this suppose the organizing and establishing of connections among various elements, including academic disciplines, research domains, study programs, courses, professors, and students.

Developing a valuable ontology for a university requires a thorough analysis of

the institution's specific requirements and goals.

For example, a well-constructed ontology could improve both teaching and research processes, streamline the organization of information spanning various academic fields, or facilitate the creation of new curricula.

In the ontology definition process, several important factors must be taken into account. These encompass determining the types of concepts and entities to be incorporated, as well as outlining their interrelationships. Moreover, careful consideration should be given to how the ontology will be implemented and used within the university.

Typically, creating university ontology involves several steps, such as defining the scope of the ontology, specifying concepts and relationships, formulating ontology models, and subjecting the ontology to testing and validation.

To ensure continued relevance and effectiveness, user feedback should be asked and regular updates made.

Our model has been designed and presented in Figure no. 1. We can see educational and data and information classes, with all their instances and properties.

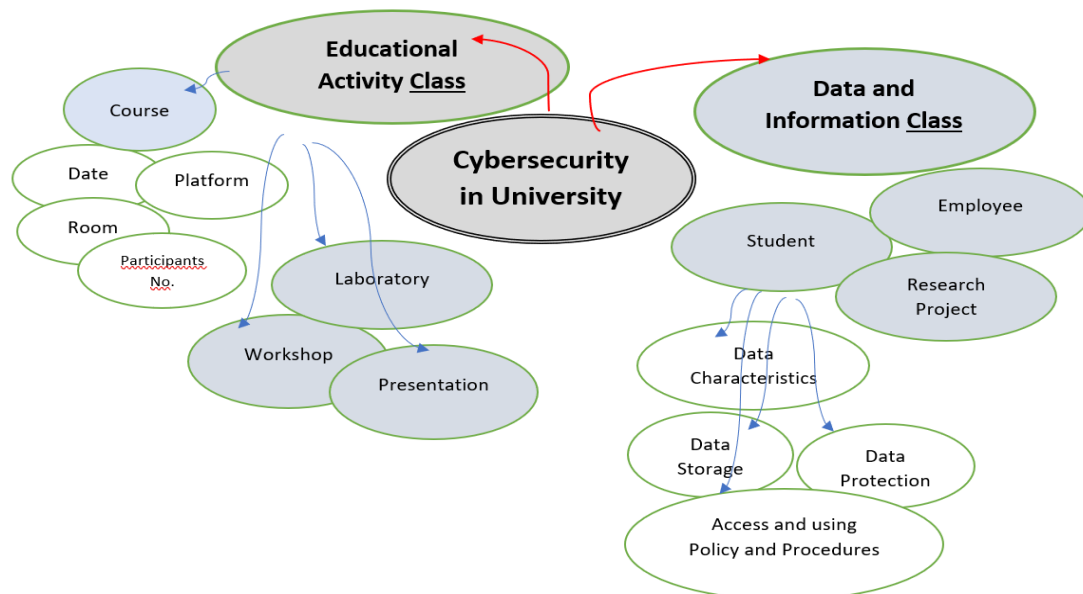


Figure no. 1: Data, information and activities in a modern university structured on ontology
(Source: Authors' contribution)

Implementing educational activities and data within a university ontology involves the following steps:

✓ *Define the Scope*. We must clearly define the scope and determine what aspects of educational activities and data we want to represent, such as courses, students, faculty, departments, and academic resources.

✓ *Select Ontology Language*. We use an ontology language (e.g., OWL or RDF) to formalize the ontology. This will provide a standardized structure for representing educational information.

✓ *Conceptualize the Model*. We must create a conceptual model that outlines the key concepts, entities, relationships and attributes relevant to the university's educational activities. This step helps in designing the ontology's structure.

✓ *Build the Ontology*: The development of the ontology is based on the conceptual model. We must define classes for entities like courses, students, professors, departments and establish properties and relationships that connect these entities, such as “teaches”, “enrols in” and “belongs to”.

✓ *Populate with Data*: In order to populate the ontology with real-world data from the university, can be done manually by inputting information or through automated processes if data sources are available in structured formats.

✓ *Incorporate Curriculum*: We can represent the university's curriculum including details about courses, prerequisites, course descriptions, and academic programs.

✓ *Include Student Information*: We can incorporate student data, such as enrolment records, academic performance, majors, and minors, into the ontology.

✓ *Faculty and Staff*: We may represent faculty and staff members, their roles, research interests, and academic qualifications.

✓ *Enable Search and Query*: It is possible to implement search and query capabilities using ontology reasoning and inference engines. This allows users to retrieve specific educational information efficiently.

✓ *Integration*: The ontology can be integrated with university systems and applications, such as student information systems, course registration platforms, and academic advising tools. This facilitates data exchange and consistency.

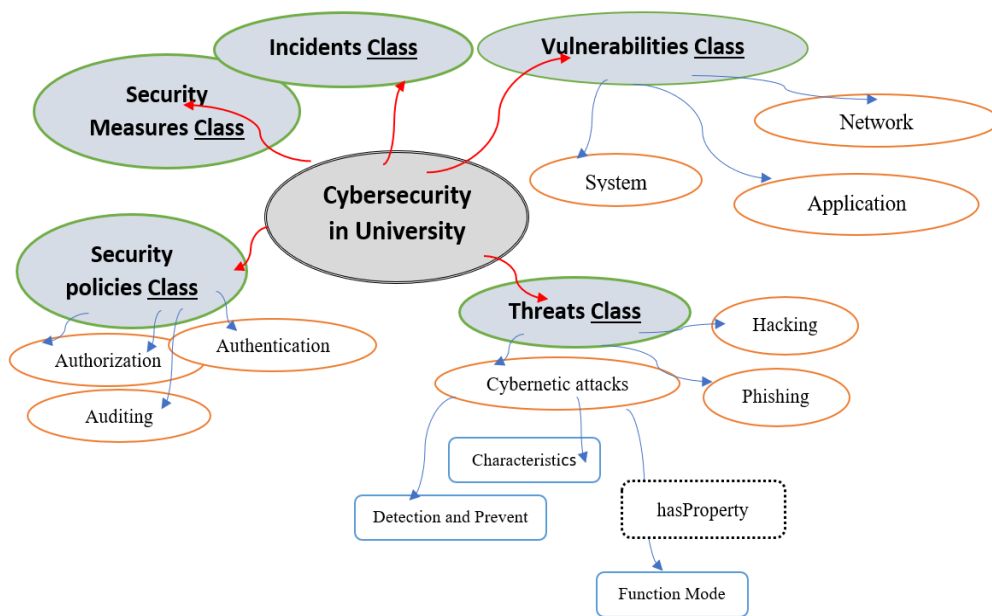
✓ *Updates and Maintenance*: the ontology must be regularly updated and maintained to reflect changes in educational programs, faculty, courses, and student records.

✓ *Semantic Interoperability*: We must ensure that the ontology adheres to semantic web standards, making it interoperable with other ontologies and linked data sources in the education domain.

By implementing educational activities and data within an ontology, a university can benefit from improved data management, enhanced search and retrieval capabilities, and better support for decision-making processes related to academics, research, and administration.

This structured representation of knowledge can also stimulate innovation in educational technology and analytics.

The cybersecurity elements are described in Figure no. 2. They need to be developed and then put into practice.



Legend: Black line: Basic level
 Green line: Concept level
 Red line: Instance level
 Arrows: Relationships level

Figure no. 2: The basic level, the concept level, the instance level, and the relationship level of the proposed ontology
 (Source: Authors' contribution)

There are several implementation languages for ontologies, the most well-known are:

1. *OWL (Web Ontology Language)* stands as a W3C standard for representing ontologies. It offers an extensive range of expressive capabilities for defining classes, properties, and complicate relationships between entities.

2. *RDF (Resource Description Framework)* serves as a language to portray resources and their interconnections through triples (subject, predicate, object). It is often used in tandem with RDF Schema (RDFS) to build simple semantic ontologies.

3. *RDFS (RDF Schema)*: RDFS extends RDF to provide functionalities for specifying classes, properties, and subclasses. Although less expressive than OWL, RDFS is preferred for designing simple ontologies.

4. *SPARQL (SPARQL Protocol and RDF Query Language)*: SPARQL is a query language designed for RDF, enabling

the retrieval and querying of data stored in RDF depositories.

5. *Turtle and N-Triples*: These RDF serialization languages facilitate the creation and interpretation of ontologies in a human-readable format.

6. *Manchester OWL Syntax*: This simplified language streamlines the process of crafting ontologies in OWL, making it more accessible, especially for persons who are not ontology experts.

7. *Protégé*: Even if is not a programming language in itself, Protégé serves as an ontology development environment offering a graphical interface for the creation and management of ontologies in the OWL language.

These applications and programming languages are used to develop and implement of ontologies, to represent knowledge and semantic data in a structured and standardized way. Choosing a programming language depends on the complexity of the ontology and its use.

To represent information about cybersecurity (see Figure no. 1) that includes the *Educational Activity Class* with its subclasses *Course*, *Laboratory*, *Workshop*, and *Presentation*, as well as the

Data and Information Class with its subclasses *Student*, *Employee*, and *Research Project* in RDF (Resource Description Framework) format, we can use the following RDF code:

```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>.
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#>.
@prefix ex: <http://example.org/>.
```

First we define classes:

```
ex:EducationalActivity a rdfs:Class.
ex:DataandInformation a rdfs:Class.
ex:Course a rdfs:Class.
ex:Laboratory a rdfs:Class.
ex:Workshop a rdfs:Class.
ex:Presentation a rdfs:Class.
ex:Student a rdfs:Class.
ex:Employee a rdfs:Class.
ex:ResearchProject a rdfs:Class.
```

Then, we define the class hierarchy:

```
ex:EducationalActivity rdfs:subClassOf ex:DataandInformation.
ex:Course rdfs:subClassOf ex:EducationalActivity.
ex:Laboratory rdfs:subClassOf ex:EducationalActivity.
ex:Workshop rdfs:subClassOf ex:EducationalActivity.
ex:Presentation rdfs:subClassOf ex:EducationalActivity.
ex:Student rdfs:subClassOf ex:DataandInformation.
ex:Employee rdfs:subClassOf ex:DataandInformation.
ex:ResearchProject rdfs:subClassOf ex:DataandInformation.
```

Finally, we instantiate ex: Cybersecurity as an educational activity.

```
ex:Cybersecurity a ex:EducationalActivity.
```

In this RDF fragment, we first define the classes and then establish subclass relationships between them, to create a class hierarchy.

The *ex: Educational Activity Class* has subclasses *ex: Course*, *ex: Laboratory*, *ex: Workshop*, and *ex: Presentation*, while the *ex: Data and Information Class* has subclasses *ex: Student*, *ex: Employee*, and *ex: Research Project*.

In the end we instantiate *ex: Cyber security* as an instance of the *ex: Educational Activity Class*, indicating that

cybersecurity is considered an educational activity in this RDF context.

6. Conclusions

There is a growing trend within universities to create security ontologies aimed at addressing both cybersecurity and physical security concerns. These ontologies serve the purpose of analyzing security risks, identifying vulnerabilities, and conceiving more efficient security strategies.

One notable advantage of employing security ontologies consists in their ability

to standardize the terminology and concepts used in security policies. This standardization proves invaluable in ensuring that all individuals involved in university security have a precise understanding of the situation and the necessary measures to protect the institution.

Furthermore, security ontologies can facilitate the development of automated security systems capable of swiftly and effectively identifying security vulnerabilities and threats. This functionality becomes particularly advantageous in larger universities managing numerous security systems and devices.

However, it's crucial to understand and take into consideration that the development and implementation of a security ontology can be a complex and time-consuming action. Equally important is the need to ensure that the ontology accurately reflects the security requirements of the university and is periodically updated to keep up with emerging threats and vulnerabilities.

In conclusion, the using of security ontologies in universities has the potential to significantly increase security efforts, but requires a careful and well-planned approach to guarantee successful implementation.

REFERENCES

Borja Rivadeneira, W.F., & Gómez, O.S. (2020). Cybersecurity Ontologies: A Systematic Literature Review. *ReCIBE - Revista electrónica de Computación, Informática, Biomédica y Electrónica*, Vol. 9, Núm. 2, 1-18.

De Rosa, F., et al. (2021). *Ontology for Cybersecurity Governance of ICT Systems*. Available at: <https://ceur-ws.org/Vol-3260/paper4.pdf>.

Dinicu, A., Oancea, R. & Bârsan, G. (2021). The Multidimensional Impact On Society Of Cyber Attacks Targeting The Energy Critical Infrastructure Sector. *Land Forces Academy Review*, Vol. XXVI, No. 4 (104).

Georgescu, T.M., & Smeureanu, I. (2017). Using Ontologies in Cybersecurity Field. *Informatica Economică*, Vol. 21, Issue 3. Available at: <https://www.revistaie.ase.ro/content/83/01%20-%20smeureanu,%20georgescu.pdf>.

Gligorea, I., Yaseen, M., Cioca, M., Gorski, H., & Oancea, R. (2022). An Interpretable Framework for an Efficient Analysis of Students' Academic Performance. *Sustainability*, Vol. 14, Issue 14. Available at: <https://doi.org/10.3390/su14148885>.

Gomes, H., Zúquete, A., & Paiva Dias, G. (2009). An Overview of Security Ontologies. *9ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI 2009)*, Portugal.

<https://www.techtarget.com/searchsecurity/definition/CVSS-Common-Vulnerability-Scoring-System>.

<https://capec.mitre.org/>.

<https://info.opswat.com/dm/>.

<https://www.techtarget.com/searchsecurity/definition/STIX-Structured-Threat-Information-eXpression>.

<https://cyware.com/security-guides/cyber-threat-intelligence/what-is-cybox-how-do-you-use-a-cybox-object-af90>.

<https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>.

https://nordlayer.com/zero-trust-security/?gclid=EAIaIQobChMItv3H2MaA_gIVgeJ3Ch3FEQA_EAAYAyAAEgLVbPD_BwE.

<https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting>.

<https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did>.

<https://www.nist.gov/cyberframework>.

Léger, M.-A., Gagnon, S., & Valverde, R. (2021). *Ontology engineering methodology for cybersecurity requirements in Business Technology Management*. Available at: https://www.researchgate.net/publication/357284585_Ontology_engineering_methodology_for_cybersecurity_requirements_in_Business_Technology_Management.

Modiba, N., Ojo, S., & Ncube, Z. (2019). An Ontology Based Model for Cyber Security Awareness Education. *Kalpa Publications in Computing, Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019, Vol. 12*, 169-179.

Pastuszuk, J., Burek, P., & Książkowski, B. (2021). Systems Cybersecurity Ontology for Dynamic Analysis of IT Systems. *Procedia Computer Science Journal, Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 25th International Conference KES2021, Vol. 192*, 1011-1020. Available at: <https://www.sciencedirect.com/science/article/pii/S1877050921015921>.