Cyberattack ontology: a knowledge representation for cyber supply chain security

Cyberattack Ontology: A Knowledge Representation for Cyber Supply Chain Security

Abel Yeboah-Ofori[1] Umar Mukhtar Ismail[2], Tymoteusz Swidurski[3] Francisca Opoku-Boateng[4]
School of Computer & Eng, Sch of Architecture, Computing & Eng, College of Computer & Cyber Science
University of West London University of East London Dakota State University
London, UK London, UK Dakota, USA
abel.yeboah-ofori@uwl.ac.uk; u.ismail@uel.ac.uk; u1966166@uel.ac.uk, Francisca.Opoku-Boateng@dsu.edu

Abstract: **Cyberattacks on cyber supply chain (CSC) systems and the cascading impacts have brought many challenges and different threat levels with unpredictable consequences. The embedded networks nodes have various loopholes that could be exploited by the threat actors leading to various attacks, risks, and the threat of cascading attacks on the various systems. Key factors such as lack of common ontology vocabulary and semantic interoperability of cyberattack information, inadequate conceptualized ontology learning and hierarchical approach to representing the relationships in the CSC security domain has led to explicit knowledge representation. This paper explores cyberattack ontology learning to describe security concepts, properties and the relationships required to model security goal. Cyberattack ontology provides a semantic mapping between different organizational and vendor security goals has been inherently challenging. The contributions of this paper are threefold. First, we consider CSC security modelling such as goal, actor, attack, TTP, and requirements using semantic rules for logical representation. Secondly, we model a cyberattack ontology for semantic mapping and knowledge representation. Finally, we discuss concepts for threat intelligence and knowledge reuse. The results show that the cyberattack ontology concepts could be used to improve CSC security.**

Keywords: *Cyberattack Ontology; Cyber Supply Chain; Cyber Security; Knowledge Representation; Threat Intelligence.*

I. INTRODUCTION

Cyber supply chain attacks rose by 42% in the first quarter of 2021 with 137 organizations reported CSC attacks ay 27 different third-party vendors [22]. with just 5% of firms assessing their cyber risks in wider supply chain context [23]. The exponential growth in CSC attack requires that we model cyberattack ontology that provides conceptual reasoning, knowledge representation, situational awareness, and threat intelligence required for strategic management understanding, decision makings and control mechanisms [1]. The conceptualization of cyberattack ontologies provides mechanisms for semantic mapping and correlations of the cyberattack in the security domain [2]. Cyber supply chain security requires direct responsibility for strategic management understanding and security governance to achieve the organizational goal [3]. However, the lack of threat intelligence and the fuzzy nature of CSC attacks has made it challenging to understand and facilitate the correlations of cyberattacks. Thus, increased security incidents and sources of vulnerabilities that exist on the various supply chain systems had led to cascading attacks. Cybersecurity attacks and risks in supply chain systems have increased exponentially leading to major breaches in most organization [4]. The report by the Department of Business, Innovation and Skills on Information security breaches, 93% of large organizations and 87% of SMEs experience a security breach in 2013, with affected companies experiencing roughly 50% more breaches than in 2012 [4]. According to the Version 2014 Data Breach Investigation report, SMEs accounts for 92 percent of total incidents analysed [5]. Thus, modelling and understanding of cyber supply chain attack have proofed challenging due to the integrated and interoperability nature of the various network nodes and the computational complexities [3]. These are due to key factors such as lack of common ontology vocabulary and semantic interoperability of threat information. Thus, we use ontology learning to conceptualize the hierarchical approach and present the relationships in the CSC security domain.

The cyberattack ontology concepts provide semantic mapping and relationships that determine attack pattern, risk and the mediated schema for threat intelligence and understanding [6]. Further, cyberattack ontology architecture can be applied to large, dynamic, complex integrated systems such as CSC systems security to meet application-specific requirements. Furthermore, it provides schematic relationships between cyberattack, threat propagations and their cascading impact on the various supply chain system network nodes. Ontology presents concepts, properties relationships and their interdependencies in a formal and structured approach. [7]. The process includes extracting relevant attack instances and threat intelligence from data to ensure consistency and accuracy in the CSC security domain. To address the issues of trust and information assurance, it is essential for organizations to map their CSC security relationships, dependencies, and vulnerabilities in an inclusive approach.

This paper explores cyberattack ontology learning to describe security concepts, properties and the relationships required to model security goal. Considering the inherent challenges, we propose cyberattack ontology that could provide a semantic mapping between different organizational business process and vendor security goals.

The contributions of this paper are threefold. First, we consider CSC security modelling such as goal, actor, attack, TTP, and requirements using semantic rules for logical representation. Secondly, we model a cyberattack ontology for semantic mapping and knowledge representation. Finally, we discuss concepts for threat intelligence and knowledge reuse. The results show that cyberattack ontology concept could be used to improve SCS security.

II. RELATED WORKS

This section discusses the related works in the CSC system security domain and cyberattack ontology concepts. Cyberattack ontology from the CSC perspective describes organizational security concepts, properties relationships and their interdependencies in a formal and structured approach for analysis and intelligence gatherings. [7] [15]. The goal of the cyberattack ontology is to extract relevant attack instances and information from data to ensure consistency and accuracy in the CSC system security concepts and for knowledge reuse in the threat intelligence domain.

A. Cyberattacks Incidents

There have been about half a billion cybersecurity breachers [8] with a various sample of cyberattack incidents that are impacting greatly on CSC systems. For instance, in April 2021, colonial pipeline network which transport about 45 percent of fuel for the US east coast was hacked. Further, inmay 2021, Meat packing giants JBS pays out 7.8m in crypto ransom after ransomware attack that affected their CSC networks systems connected in Australia, Canada and USA and other subsidiaries [24]. In March 2017, an employee at a service provider firm accidentally loaded an unencrypted database containing names, address, and social security numbers on 20,000 customers to public service including usernames and passwords for employee accounts. Further, in 2018, an error by an IT service provider exposed cloud storage data, and FTP credentials, secret keys and passwords when an employer deployed an instance of an apache airflow server on the system of clients, without securing it with a password [8]. Furthermore, in 2018, hackers accessed the frontend server of an AI and chatbot company and inserted a vulnerability that skimmed customers payment card details through ticket master [8].

B. Cyberattack Ontology

Oltramari (2014) outlined the underpinning of ontology secure operations in cyberspace by presenting an ontology framework using descriptive ontology for linguistic and cognitive engineering [9]. Asim et al (2018) surveyed ontology learning techniques and applications by classifying linguistic, statistical, and logical learning techniques using various algorithms including hierarchical clustering, ARM, and contrast analysis [7]. Mozzaquatro et al. (2019) proposed architecture of the IoT security ontology framework to using an adaptive security model to improve secure information and decision makings for industrial systems [6]. Doyikova & Fedorchenko (2019) proposed ontology metrics for cyber security assessment that determines the concepts and relationships between primary features of initial security data [10]. Aviad et al. (2015) proposed a semantic approach to cyber security ontology that can integrate security concepts knowledge representation and sharing for defence prioritization [1]. Iannacone et al. (2007 developed a knowledge graph for cyber security ontology that provides an organizational schema for information gathered from structured and unstructured data source [11]. Obst et al. (2012) developed an ontology for the cyber security domain that describes how malware standards, schemas and terminologies contribute to initial malware effort [12]. Salem & Wacek (2015) constructed cyber security defence ontology through a targeted attack premonition using integrated operational data to extracted data from across enterprises into a fully linked semantic graph in real-time [13]. Kotenko et al. (2013) proposed a novel approach to ontological representation using security metrics and evaluation as a core component for decision support systems in implementing countermeasures [14].

The related works are all relevant and contribute towards the improvement of cyberattack and cyber security knowledge representation using ontology concepts. However, none of the works considered the modelling cyberattack ontology from cyber supply chain security perspective to improve security.

III. APPROACH

The proposed approach considers the cyberattack model within the CSC domain using ontology concepts [1] [12]. Cyberattack ontology concepts provide knowledge representation and support the understanding of threat properties. We consider properties such as goal, actors, Tactics, Techniques and Procedure (TTP), attack, vulnerability, and CSC requirements for the cyberattack ontology modelling.

A. The rationale for Implementing Cyberattack Ontology

The rationale for the paper is based on the premise that the cyberattack phenomenon includes a lot of uncertainties making the CSC threat landscape unpredictable. Additionally, due to the varying organizational goals and dynamic requirements, various integrations, varying business processes, and delivery mechanisms, predicting cyberattacks in CSC from an organizational perspective has been challenging. To address these challenges, we consider the CSC cyberattack modelling approach using ontology concepts for knowledge representation and reuse within the CSC domain [15] [16] as shown in Figure 1.

VI. IMPLEMENTATION

This section provides an overview of the proposed approach from conceptual and ontological perspectives and the processes used for knowledge representation

for the cyberattacks and various compromises. A Cyber Supply Chain Compromise attack is the manipulation of products delivery mechanisms prior to receipt by a final consumer [17]. First, we model cyberattack ontology concepts CSC using concepts such as goal, actor, attack, TTP, and requirements [21] using semantic rules for logical representation or the CSC system security. Secondly, we model a cyberattack ontology for semantic mapping and knowledge representation. Finally, we discuss concepts for threat intelligence and knowledge reuse. By using semantic rules and logical representation of the concepts, we can create a graphically visualize the concepts to aid automated assessment, analysis, and processing of data to using ontology development techniques. Hence, Protégé is used to develop the ontologies because it provides an intuitive editor for ontologies and other extensions for ontology visualization and rule generation. Protégé is one of the most widely used free, open-source ontology editor that was developed at Stanford University [16] as discussed in the following.

A. Cyberattack Ontology Semantic Mapping and Rule Set

Goal: The goal describes the aim of an organization. Identifying goal assisting in determine what are required to achieve Organisational goal and Security goal. For instance, an organisational goal may require ensuring product quality, reliable and secure services to vendors and consumers. Security goal will ensure that the systems are confidentiality, integrity, availability, of the product or services. The security goal emphasises more on adversary goals of attacking and aborting the main organisational goal. The threat actor goal is to deploy attacks on the CSC system to exploit existing vulnerabilities manipulate, divert, exfiltrate and take command and control of the system and assets. [18] [19].

Figure 1. Semantic Mapping and Rule Set for Goal

Actor: An actor describes an entity that has goals and intentions within the system or within the organizational setting. Actors can be recognized either by their password, identity, responsibilities or privileges. The actor's concepts legitimate system users include users such as system, internal and external. Suppliers and distributors such as external organizations and third-party vendors. Threat actor such as illegitimate actors or system users that may be internal and external.

Threat Actors are the characterisations of malicious actors or adversaries representing a cyberattack threat including presumed intent and historically observed behaviour [18]. Properties of Threat Actor are identified by their motives, intent, capabilities, and resources. The threat actor as an entity can breach or compromise the supply chain system such as a person, user account or processes that are required to perform system functions. The threat actor can have a one-to-many or many-to-many relationship within the CSC system that may cause vulnerabilities and risks. We identified threat actors through their capabilities and identity such as privilege, the intents, type of password used, observed user behaviour and patterns deployed over time, history, and motives of the actor on the supply chain.

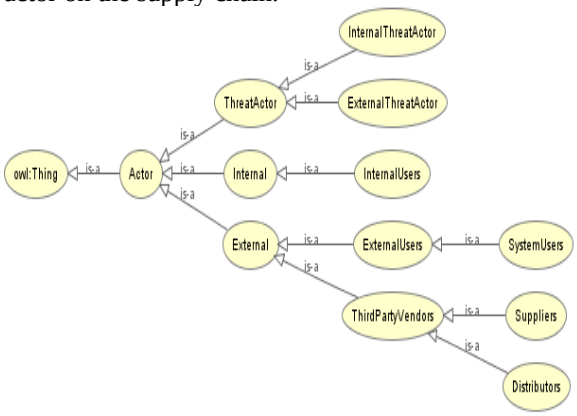

Figure 2. Rule Set for Actor and Threat Actor

Vulnerabilities: flaws and loopholes that a threat actor or a threat agent can exploit. Two key areas of vulnerable spots include internal or external (third-party) withing are human vulnerabilities that may be exploited. The rule set represents the semantic mappings that express relations between subsets of entries to external factors. The vulnerable spots could be identified from various sources including the software, network, website, user, processes, application, and configurations or third-party vendor systems [20].

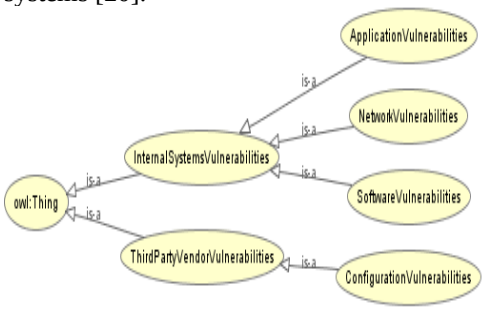

Figure 3. Rule Set for Vulnerability

Attack: Any deliberate action or assault on the supply chain system with the intent to compromise the product, or service, business processes, procedures, and delivery channels, information flows. Properties of attack include attack type, pattern, prerequisite and vector. The type of cyberattack or penetration and type of cybercrime or manipulation determines the nature of exploits on the system and that information as indicators of compromise. The attack pattern provides an abstraction mechanism for describing how a type of observed attack is executed or deployed. For instance, Spear phishing, Cross Site Scripting, Session Hijacking, RAT, SQL Injection, malware and ransomware may require different attack pattern. Prerequisite describes informs gathered that the CSC that assist the great actor's attack intent. For instances, using reconnaissance to identified vulnerable spots to a knowledge of attack tool, method, opportunity and motive. Attack vector provides the various trajectories to deployed cyberattacks and gains access to the CSC system. For instance, threat actor initiate XSS, session hijacking or RAT attack on vendor network to gain access, then penetrate and cascade to other systems.

Figure 4. Semantic Mapping and Rule Set for Attack Types

Tactics, Techniques, and Procedures (TTP) describes the adversary behaviour or types of operations (STIX, 2019). Threat actors TTP leverages on specific adversary capabilities, behaviours, and exploits used on the victim's systems. The threat actor uses TTPs that acts as a schema for the attacker goal. They are parameters used to express an indication of an attack. The properties of TTP includes tactics, techniques, and procedures.

Tactics describe how threat actors operate during the various attack campaigns. For instance. A remote access trojan (RAT) attack requires that the threat actor carries out reconnaissance for initial intelligence gathering on key targets. Reconnaissance requires tactical knowledge regarding how the attack information is gathered from vulnerable spots, how the initial compromises will be conducted, the privilege escalation process, and how to perform lateral movements persistently.

Techniques: The different approaches the threat actor used to deploy to gain access to ease the initial means of compromising the system including the use of social engineering techniques to gain access. The skills to insert malware in an email attachment in a spear phishing attack, the software tools, and the capabilities and knowledge of the attacker.

Procedures: These are documented methods and steps that are grouped together and are used uniquely to perform an attack. Procedures may vary depending on the actor goal, purpose, and nature of the attack that is being deployed. For instance, procedures required for Malware attack may differ from Ransomware and that of APT attack. Threat actors may require different access rights, privileges and configuration mechanisms to determine what could be exploited.

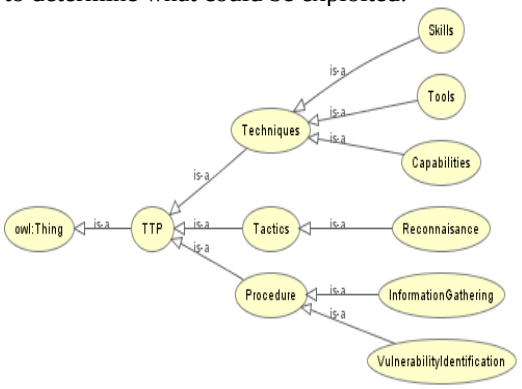

Figure 5. Tactic Techniques & Procedures (TTP) Rule Set

Requirements: These are the various constraints and expectations of how the systems should function to support the CSC system uses and business objectives. The requirements concepts include properties such as organizational requirements, business requirements, system requirements, user requirements and operational requirements Organizational requirements describe high-level objectives required to achieve the organisational goal. For instance types of users, user ID, acceptance criteria, and data owners. Business requirements specify customer demands and expectations in line with the system requirements. Systems requirements for a specific application, software, hardware architecture and the technical requirements that describe the constraints, assumptions and acceptance criteria and the external audit requirements. generated during the requirements engineering phase that forms the basis for the system. User requirements capture operational constraints of the actors (including threat actors) and service constraints of the supply chain systems to determine organisational goal and security goal. Operational requirements parameters and configurations used to establish operational processes amount stakeholders. Technical Factors in CPS Requirements: Cyber Physical Systems development is a highly abstract system that combines the physical, digital and human elements to enhance business processes.

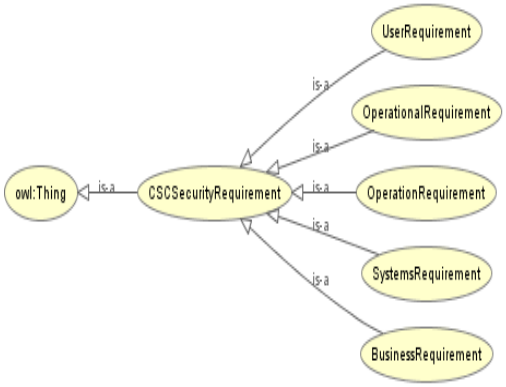

Figure 6. Semantic Mapping and Rule Set for Goal

B. Cyberattack Ontology Conceptual Model

The proposed conceptual model for cyberattack ontology attempts to clarify the implication of cyberattacks from uncertain and ambiguous terms for knowledge representation and prevent different interpretation. The model presents a semantic mapping between different attack concepts, properties and the relationships required for vendor networks on supply inbound and outbound chains security goals has been inherently challenging. This paper explores cyberattack ontology learning to describe concepts required to model security goal. We consider ontology learning for goal, CSC requirements, actor, threat actor, CSC, TTP, attack and vulnerability. The goal represents what an organization wants to achieve. That may be product development or service-oriented and may access the CSC system to engage with suppliers, distributors and third-party vendors to be the goal. The actor relies on the CSC requirements and various configurations to achieve the goal. For instance, the threat actor may want to abort the business process through a malware attack, information flow using denial of Service attack (DoS), steal information through industrial espionage attack or manipulate delivery channels using command and control attack. The threat actor may use TTP to deploy attack to exploit the vulnerable spots. The extent of vulnerabilities that could be exposed to the CSC requirements determines the cascading impact of a cyberattack on the CSC system. The risk of a potential attack and its cascading impact from a threat actor poses a constant challenge. The probabilities of cyberattacks being initiated on the supplier inbound and outbound from a vendor network are high due to misconfigurations and represent a single point of failure, especially in small SMEs. We use ontology concepts to identify the risk of a cyberattack on the CSC, we look at the vulnerabilities, threats, actors, and attack vectors that could be exploited on the cyber inbound and outbound chains. For instance, consider the threat of an adversary deploying a drive-by compromise attack on the vendor systems to breaching the network. Buying software off the shelf poses vulnerability factors including the risk of the software developer inserting malware or spyware into the software purchased by a vendor. The CSC requirements assist in identifying constraints on the supply inbound and outbound chains and consider the level of impact on the organizational goals [3] [21].

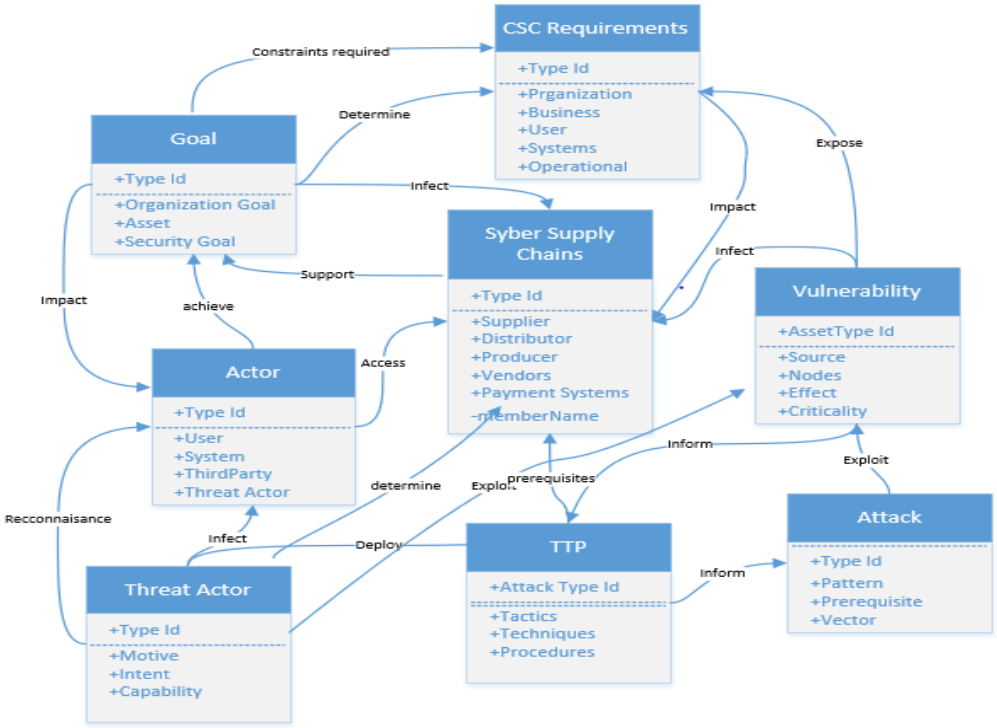

Figure 7. Proposed Conceptual Model of Cyberattack Ontology

V. DISCUSSIONS

Cyberattack ontology act as a link that connects the concepts with the threat data used cyber security information and incident management lifecycle to assist in predicting potential cyberattacks. For instance, by the ontological representation of concepts and data, we could answer the following questions “what threat

agent can a threat actor use to compromise an asset on the supply chain system? “What controls are required to mitigate a threat-agent?” etc. First-order logic provides one of the fundamental logical formalization techniques used for knowledge representation and baseline content to support CSC interoperability and ensure security best practices. The benefits of first-order logic according to [16] are that it allows the description of concepts, objects or things that have an individual identity, and to construct logical formulas around these objects using predicates, variables, functions, and logical connectives.

Cyberattack schemas provide structural interoperability that could be vulnerable to human error, interpretations, and configurations in a logical relationship. We used the protégé tool to model the relationships that enable interoperability in a machine interpreted method that expresses the meaning, structure and syntax of cyberattacks incidents and its cascading impacts in the CSC domain. The natural language statements or rules regarding the cyberattacks ontology concepts in the CSC domain can be expressed in terms of coherent sentences with appropriate predicate and function symbols as explained in the model.

Comparatively, none of the related works considered modelling cyberattack ontology from cyber supply chain security perspective to improve security.

VI. CONCLUSION

In this paper, we have used semantic rules and logical representation of cyberattack ontology concepts to create graphically visualize concepts to aid in automated assessment, analysis, and processing of cyberattacks for knowledge reuse in CSC security. The protégé tool was used to develop the ontologies as it provides an intuitive editor for ontologies and other extensions for ontology visualization and rule generation. The paper has shown that cyberattack ontology concepts complement structural interoperability and knowledge representation in the CSC systems security domain. Future works will focus on cyberattack modelling using a case study to determine the attack methods and homomorphic encryption to improve security.

REFERENCES

[1] A. Aviad, K. Wecel, and W. Abramowicz. “The Semantic Approach to Cyber Security Towards Ontology Based Body of Knowledge” Conference Proceedings of the 14th European Conference on Cyber Warfare and Security (ECCWS). 2015.

[2] K. Arbanas, and M. Cubrilo. “Ontology in Information Security” Journal of Information and Organizational Science. JIOS, VOL. 39, NO. 2. 2015.

[3] A. Yeboah-Ofori, and S. Islam, “Cyber Security Threat Modelling for Supply Chain Organizational Environments.” MDPI. Future Internet. 11, (3), 63, March 2019. doi: 10.3390/611030063.

[4] Department of Business Innovation & Skills. Information Security Breaches Survey. Technical Report. PWC. 2013.

[5] Verizon Data Breach Investigations Report. “Identifies More Focused, Effective Way to Fight Cyberthreats”. 2014

[6] B. A. Mozzaquatro, R. Melo, C. Agostinho and R. Jardim-Goncalves, "An ontology-based security framework for decision-making in industrial systems," IEEE Xplore. *2016. 4th International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*, 2016, pp. 779-788.

[7] M. N. Asim, M. Wasim, M. U. G. Khan, W Mahmood, and H. M. Abbasi. “A survey of ontology learning techniques and applications. Database”. 2018, 1–24. doi: 10.1093/database/bay101.

[8] Bitsight. “How to Protect Your Digital Supply Chain & Improve Third-Party Risk Management”. www.bitsight.com.

[9] A. Oltramari, L. F. Cranor, R. J. Walls, and P. McDaniel. “Building Ontology of Cyber Security”. Semantic Scholar. STIDS. 2014.

[10] E. Doynikova, A. Fedorchenko, and I. Kotenko. “Ontology of Metrics for Cyber Security Assessment” ACM. ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security. No. 52. Pages 1–8. 2019. https://doi.org/10.1145/3339252.3341496.

[11] M. Iannacone, S. Bohn. G. Nakamura, J. Gerth, K. Huffer, R. Bridges, E. Ferragut, and J. Goodall. “Developing an Ontology for Cyber Security Knowledge Graphs” ACM. CISR '15: Proceedings of the 10th Annual Cyber and Information Security Research Conference. No. 12. Pages 1–4. 2015. https://doi.org/10.1145/2746266.2746278

[12] L. Obrst, P. Chase, and Markeloff, R. “Developing an Ontology of the Cyber Security Domain”. Semantic Scholar. *STIDS*. 2012.

[13] M. B. Salem, and C. Wacek. “Enabling New Technologies for Cyber Security Defense with the ICAS Cyber Security Ontology.” Semantic Scholar. *STIDS*. 2015.

[14] I. Kotenko, O, Polubelova, I. Saenko, E. Doynikova, “The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems”. ACM. ARES '13: Proceedings of the 2013 International Conference on Availability, Reliability and Security. Pg 638–645. 2013. https://doi.org/10.1109/ARES.2013.84.

[15] A. Yeboah-Ofori, U. Ismai, S. Islam, H. Mouratidis, and S. Papastergiou. “Cyber Supply Chain Threat Analysis and Prediction using Machine Learning and Ontology”. In: Maglogiannis I., Macintyre J., Iliadis L. (eds) Artificial Intelligence Applications and Innovations. AIAI 2021. IFIP Advances in Information and Communication Technology, vol 627. Springer, Cham. https://doi.org/10.1007/978-3-030-79150-6_41

[16] N. F. Noy, D. L. McGuiness. “Ontology Development 101.: A Guide to Creating Your Own First Ontology. Stanford.

[17] CAPEC-437: Supply Chain. Common Attack Pattern Enumeration and Classification: Domain of Attack 2018. https://capec.mitre.org/data/definitions/437.html MITRE.

[18] MITRE. Threat Based Defense. Understanding an Attackers Tactics and Techniques is Key to Successful Cyber Defense. 2018.

[19] STIX: Assets Affected in an Incident. http://stixproject.github.io/documentation/idioms/affected-assets/

[20] CWE. Common Weakness Enumeration. Supply Chain Risk Management and Due Diligence. 2018.

[21] A. Yeboah-Ofori *et al.*, "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," in *IEEE Access*, doi: 10.1109/ACCESS.2021.3087109.

[22] Identity Theft Resource Cener (ITRC). “Troubled rise in supply chain cyber security”. 2021.

[23] Departments for Digital, Cultural, Media and Sports (DCMS) 2021. Survey.

[24] France 24.”US Subsidiary of Meat-packing giant JBS hit by cyberattack”. 2021 .