Toward a Unified Cybersecurity Knowledge Graph: Leveraging Ontologies and Open Data Sources

Adam Boyer
Department of Computer Science
Angelo State University
San Angelo, Texas
aboyer@angelo.edu

Erdogan Dogdu
Department of Computer Science
Angelo State University
San Angelo, Texas
edogdu@angelo.edu

Jason Watson
Department of Computer Science
Angelo State University
San Angelo, Texas
jason.watson@angelo.edu

Roya Choupani
Department of Computer Science
Angelo State University
San Angelo, Texas
roya.houpani@angelo.edu

Jordan Wade
Department of Computer Science
Angelo State University
San Angelo, Texas
jwade9@angelo.edu

Alexander Ametu
Department of Computer Science
Angelo State University
San Angelo, Texas
aametu@angelo.edu

***Abstract*—The cybersecurity field is very heterogeneous with the ever-growing digital cyberspace and the increasing volume of big data produced in the field. It is therefore difficult to overcome many of the security challenges with manual solutions. Automation and intelligent cybersecurity solutions are both promising tools to overcome common security challenges, however, they require robust data and knowledge management. Today, Knowledge graphs (KG) are widely used in many intelligent system solutions, including the cybersecurity field. However, the efforts to build KGs in many cybersecurity areas are narrowly focused, and therefore it is difficult to unify and integrate these otherwise very useful solutions. Earlier efforts in unifying the cybersecurity knowledge using common ontologies have not generalized their approach to provide a unified solution for cybersecurity challenges. Here, we attempt provide a renewed approach to building a Unified Cybersecurity Knowledge Graph (UCKG), using the Unified Cybersecurity Ontology (UCO), that integrates structured and unstructured open data sources in an automated fashion. With this paper, we hope to pave the way toward a Unified Cybersecurity Knowledge Graph (UCKG) and its utilization in intelligent cybersecurity solutions.**

***Index Terms*—Cybersecurity ontology, cybersecurity knowledge graph, intelligent cybersecurity, Unified Cybersecurity Ontology, Unified Cybersecurity Knowledge Graph**

I. Introduction

There has been an explosion of data and computational power in recent years, and almost every domain now benefits from big data, data science, machine learning, and AI in some capacity. Cybersecurity is no exception and it benefits tremendously from big data [14]. Big data and data-driven AI transforms the cybersecurity domain tremendously. We see more data-driven and intelligent solutions brought to the cybersecurity field in all areas, from security assessment, threat discovery, and all sorts of intelligent security operations [2], [10].

The current cybersecurity landscape is full of data and knowledge pouring from many resources, from government agencies to industrial bodies. The heterogeneous nature of this data space underlines the need for a unified knowledge resource that can be used to provide comprehensive and intelligent cybersecurity solutions. Previous research has focused on solutions in specific areas such as malware detection, intrusion detection, etc. While efforts to solve specific issues plaguing the cyberseurity domain is useful, a unified solution is needed to provide comprehensive cybersecurity solutions.

The number and breadth of cybersecurity threats is ever-changing. Up-to-date information on the latest threats is needed to maintain the usefulness of any cybersecurity solution. With distributed sources of information, it is difficult to correlate resources in real time without a unified knowledge source. There needs to be comprehensive, integrated, and up-to-date source of information available that connects disparate resources into a single pane of glass.

Ontologies and knowledge graphs are important tools in unifying the distributed and disparate cybersecurity information sources and data. There has been efforts toward to this goal earlier [1], [3], [9], but these early efforts failed to complete their objectives and abandoned the initiatives early. Now, with the increasing interest in the utilization of knowledge graphs in all types of intelligent solutions, there is a chance to start this over and provide a comprehensive and working data integration solution for cybersecurity. This time the possibility of success is higher, since the field has matured in the last few years in a number of fronts. First, KGs are being utilized and has been shown to provide success in many machine learning and intelligent automated solutions. So, there is an opportunity to utilize KGs in the cybersecurity field, there has been many efforts alerady, we just have to show a working unified solution. Second, the cybersecurity field has grown tremendously with the growth and availability of data. Now is the time to harvest. There is need for a comprehensive solution that integrates big data using KG representation and reasoning. Third, we have reason to believe that the earlier efforts in unified cybersecurity ontologies and vocabularies

did not get wide adoption due to the immaturity of the field and the up and coming age of AI. Now, with big data and sophisticated ontology solutions, we believe there will be many intelligent applications taking advantage of KGs for many different scenarios, from risk assessment to cyber threat intelligence modeling, cyber readiness and defense, and more.

In this paper, we address the need for a unified cybersecurity knowledge graph and present a method for building one using the Unified Cybersecurity Ontology (UCO) and its enhancements. We envision integrating scattered data sources such as Common Vulnerabilities Enumeration (CVE), Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC), Common Platform Enumeration (CPE), Common Vulnerability Scoring System (CVSS), and After Action Reports (AARs). This is a more comprehensive list of resources than earlier efforts. Our UCKG is also extensible, new data sources can be added and integrated using a common ontology. We also present a vision for how the ontology and accompanying KG can be utilized in intelligent cybersecurity operations.

In section II we present the previous work in this area. We review the ontology we are using and the integration approach in section III and then present the methodology we are using to build the UCKG in Section IV. Section V reviews the list of structured and unstructured data sources we are using to integrate and build the UCKG. Section VI presents an approach for visualizing and exploring the UCKG which we plan to integrate into a comprehensive application with this project. There could be many intelligent applications benefiting from and using the UCKG, and we present a glimpse of those in section VII. We finally conclude and point to future work in section VIII.

II. Related Work

Cybersecurity knowledge graphs (CKG) have been getting a lot of attention recently, due to the cybersecurity field using and benefiting from big data and intelligent solutions. CKGs are utilized to represent knowledge obtained from cybersecurity field. They use a graph-model to represent concepts, entities, and artifacts as nodes, and the relationships between them as edges. CKGs are used to represent complex cybersecurity knowledge and data in a simple and unified framework for easy management, access, and maintenance. CKGs also allow us to develop sophisticated AI-based intelligent cybersecurity solutions.

Zhao et al surveyed the area of CKG construction [8]. They reviewed studies constructing (1) general CKGs that can be used in many types of applications, and (2) those CKGs that are constructed for specific application areas, such as intrusion detection, malware detection, risk assessment, etc. They also point to the gap between abstract CKG information and actual log data, as well as the scarcity of abnormal data within.

There are many uses of KGs in cybersecurity and many studies have developed and utilized CKGs for different purposes. For example, Piplai et al [11] presented a system for extracting information from "After Action Reports" (AAR), building a cybersecurity knowledge graph (CKG) and fused information coming from multiple AAR reports and resources, therefore presenting an integrated view of threat intelligence.

STIX [3] is an earlier effort from MITRE corporation in standardizing cybersecurity vocabulary. However, STIX is based on XML, a legacy standard for building semantic knowledge bases or knowledge graphs. STIX also incorporated vocabularies from other standards, therefore it was valuable effort in the path towards a unified ontology. The UCO also incorporates and maps concepts and entities from STIX [9].

STUCCO[1] is yet another effort in providing a comprehensive CKG. It is an organized ontology schema collecting information from many structured and unstructured data sources [1]. GitHub repository[2] of the project shows little to no activity since its release.

The Unified Cybersecurity Ontology[3] (UCO) [9] is one of the latest ontologies to support information integration in cybersecurity, incorporating heterogeneous data and knowledge schemata from disparate cybersecurity systems and commonly used cybersecurity standards for information sharing and exchange. The UCO can be used to represent temporal (time) information and therefore promising reasoning capabilities. It can be used in information extraction from textual reports, blogs, and similar data sources, and thus speed up the process of information exchange and developing countermeasures against cyber attacks. The latest released version the UCO 1.5 [4] includes more than 500 classes and 900 properties. According to a recent study by Bolton et al [12] the most commonly used ontology for building CKGs is UCO, so it is adopted well in the community.

SEPSES [20] is a recent CKG effort to develop a comprehensive dataset with data collected from many open data sources, such as CVE, CWE, CAPEC, CPE, using a standard ontology like UCO. A bottom-up approach is followed in order to build the SEPSES CKG using National U.S. Vulnerability Database (NVD) and a set of online security resources. They also demonstrated the effectiveness of SEPSES by two use case studies in vulnerability assessment and intrusion detection. However, there is no activity in their project[5] since its inception, version 1.1.0.

It is clear that there is a strong need for a unified CKG, both for providing a unified ontology or vocabulary to integrate disconnected cybersecurity knowledge sources, and also for collecting the artifacts, actual data representing the cybersecurity related domain information and data. Here we attempt to do that with both structured and unstructured open data sources and a standard ontology, like UCO.

Liu et al. [2] pointed out that although there has been a large number of work in building CKG for different purposes,

[1] https://stucco.github.io/

[2] https://github.com/stucco

[3] https://github.com/Ebiquity/Unified-Cybersecurity-Ontology

[4] https://github.com/Ebiquity/Unified-Cybersecurity-Ontology/blob/master/uco_1_5.owl

[5] https://github.com/sepses/cyber-kg-converter

there is limited work on how to utilize CKG in applications to solve real-world problems.

Sarker et al. presented the most recent developments in AI-driven cybersecurity [10]. They review the most popular studies in the area of machine learning, deep learning, and natural language processing toward intelligent cybersecurity decision making, analysis, and management. They also discuss research opportunities in knowledge representation and rule-based expert system modeling.

We plan to provide a number of use cases as future work to showcase the utilization of the UCKG in intelligent cybersecurity solutions.

III. Cybersecurity Ontology, Integration, and Project UCKG

Ontologies are an essential components of CKGs. Ontologies allow subject matter experts and modelers to create an agreed-upon structure and vocabulary for sharing information in different domains [18]. They allow machines to better understand the information contained in a knowledge graph and to make inferences. An example of a widely adopted ontology is the Financial Industry Business Ontology[6], or FIBO, which was created as a standard of terms and relationships used in financial institutions.

The Unified Cybersecurity Ontology (UCO) is the most complete and comprehensive at the time of this writing [9]. The UCO ontology includes the following classes for categorizing cybersecurity entities: Means, Consequences, Attack, Attacker, AttackPattern, Exploit, Exploit Target, and Indicator. These classes were derived from cybersecurity standards such as CVE, CWE, CAPEC, CPE, and CVSS. The UCO was meant to be a semantic extension of the STIX project, which was very comprehensive, but did not allow reasoning and used the legacy XML format.

Because the UCO is based on current cybersecurity standard metrics, we believe that it is a adequate ontology for integrating the current publicly available cybersecurity information into a "Unified Cybersecurity Knowledge Graph" (UCKG). The goal of our project, UCKG, is to use the UCO ontology to integrate CVE, CWE, CAPEC, CPE, and CVSS into a knowledge graph in an automated way. The UCO's vocabulary will be used to dynamically map and transform data into a unified, connected, integrated cybersecurity knowledge graph, which will be a reference for future intelligent cybersecurity applications.

IV. Methodology

We take inspiration for the architecture of UCKG and our knowledge graph creation from the methods described by Kiesling et al [20] for their SEPSES knowledge graph. Unlike the SEPSES project, we follow the Unified Cybersecurity Ontology proposed earlier. We also adopted an open-source script described by Sharma et al [21] and modified it for the dynamic creation of Cypher queries. Figure IV shows a high-level overview of our UCKG creation and automated maintenance process.

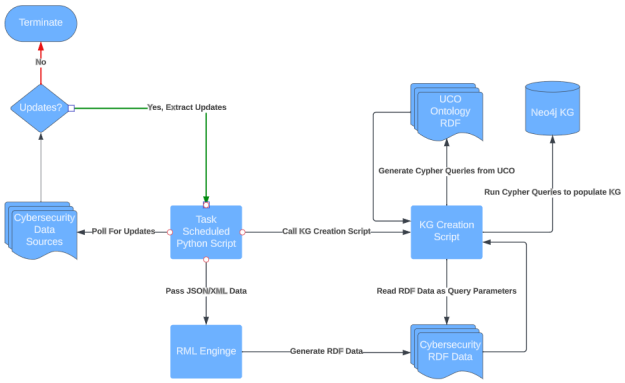


Fig. 1. Knowledge Graph Creation Flow.

A. Automated Data Acquisition

Multiple scripts are written to download the initial data from CVE, CWE, CAPEC, CPE, and CVSS. Once the initial construction of the knowledge graph is complete, a task scheduler is used to poll the respective data sources twice a day for updates.

B. Transform Data to RDF

The data received from the data sources comes in the form of JSON and XML. We transform the data into RDF, using Turtle format. The RML mapping language[7] is the language used for mapping structured data to RDF format. We then create these mappings and process the data acquired using a simple RML engine RMLStreamer[8].

C. Dynamic Creation of Cypher Queries

Our project utilizes Neo4j[9] as our triple store to maintain the UCKG. Neo4j uses Cypher[10] as its query language. We developed scripts to dynamically create Cypher queries, based on the structure of the UCO, to insert or update information in the UCKG.

D. Neo4j Knowledge Graph Creation

As previously stated, Neo4j is used as our graph database or triple store. Once the Cypher queries are created, the same script will call the queries to populate the knowledge graph. We will run our queries in batches to allow for logging and monitoring of the process.

[6]https://edmcouncil.org/frameworks/industry-models/fibo/

[7]https://rml.io/docs/rml/introduction/
[8]https://github.com/RMLio/RMLStreamer
[9]https://neo4j.com/
[10]https://neo4j.com/developer/cypher/

V. Cybersecurity Data Resources

Many of the publicly available cyber security data sources are linked to each other by properties or object IDs. Figure V depicts how these different data sources are linked together. We briefly describe each data source below.

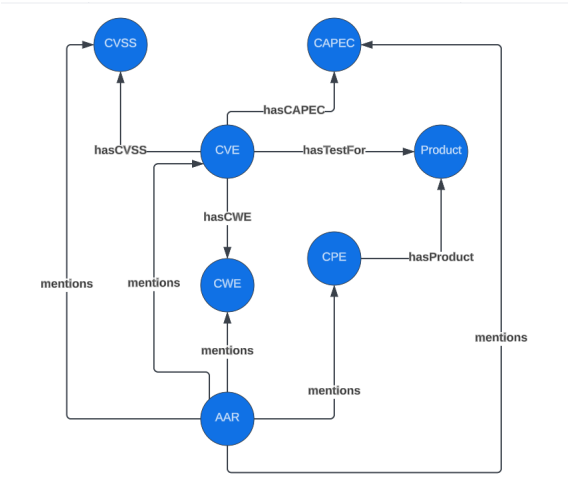


Fig. 2. Data source connected diagram.

A. Common Vulnerabilities Enumaration (CVE)

The Common Vulnerabilities List, or CVE, is a publicly available catalog of known cybersecurity vulnerabilities. The list first became publicly available in September 1999. Analysts and researchers can access the CVE List via a direct download on the official CVE website[11], or through the CVE API hosted on the NIST website[12]. Currently, there is a total of 215095 CVE records available. A CVE record will be assigned a CVE-ID by a CVE Numbering Authority (CNA). CVE records contain a description of the vulnerability, references to better understand the vulnerability, and the name of the CNA. CVE records are crucial for security experts and vendors to recognize and mitigate security vulnerabilities.

TABLE I
Important CVE Fields

Important CVE Fields	
Field	***Example***
CVE-ID	CVE-2023-5257
Description	A vulnerability was found in...
References	https://vuldb.com/?id.240866
Assigning CNA	VulDB
Date Record Created	20230929

B. Common Weakness Enumeration (CWE)

The Common Weakness Enumeration, or CWE, is a list of common software and hardware weakness types. There are currently over 600 categories in the CWE list. CWEs include useful information such as a description, relationships to other CWEs, applicable platforms, and many more The CWE list is community-developed, and was first released in 2006. It can be accessed via a direct download from the CWE website[13]. Efforts are currently being taken to standardize the CWE into a JSON-based REST API[14], but as of the time of this writing, it is not complete. The CWE is a useful tool for researchers and analysts to recognize common flaws that may affect software or hardware.

TABLE II
Important CWE Fields

Important CWE Fields	
Field	***Example***
Weakness ID	787
Weakness Name	Out-of-bounds Write
Description	The product writes data past ...
Relationships	ChildOf CWE-119
Applicable Platforms	C (Often Prevalent)

C. Common Attack Pattern Enumeration and Classification (CAPEC)

The Common Attack Pattern Enumeration and Classification, or CAPEC, was initially established by the U.S. Department of Homeland as an effort to identify and share known attack patterns in the cybersecurity community. CAPEC was initially released in 2007 and allows for public contributions to its knowledge base. There are currently 559 total attack patterns listed by CAPEC. CAPEC records list a brief description of the attack pattern, severity of the attack, possible mitigation methods, related CWEs, and more. The CAPEC list can be accessed via a direct download from the CAPEC website[15]. Efforts are currently being taken to standardize the CAPEC into a JSON-based REST API[11], but as of the time of this writing, it is not complete. The CAPEC list is needed by analysts and researchers to be able to recognize the signs of a possible attack.

TABLE III
Important CAPEC Fields

Important CAPEC Fields	
Field	***Example***
Category ID	156
Category Name	Engage in Deceptive Interactions
Summary	Attack patterns within this category ...
Membership	MemberOf ID 1000
Submission Date	2014-06-23

D. Common Platform Enumeration (CPE)

The Common Platform Enumeration, or CPE, is a publicly available dictionary of known systems, software, and packages. Naming of entities in the dictionary is based on the

[11]https://www.cve.org/
[12]https://nvd.nist.gov/developers/products
[13]https://cwe.mitre.org/index.html
[14]https://cwe.mitre.org/documents/CWE-CAPEC_Rest_API_Working_Group.pdf
[15]https://capec.mitre.org/index.html

Uniform Resource Identifier, URI, format. Some important information contained in the CPE are CPE version, part or type (i.e. applications, hardware, or operating systems), vendor, and product. The CPE dictionary is continually being updated, with over 16,000 additions made in just September of 2023. Analysts and researchers can access the CPE dictionary via a direct download[16] or through the CPE API hosted on the NIST website[2]. The CPE dictionary is essential for cybersecurity experts to have a structured way of identifying entities.

TABLE IV
IMPORTANT CPE FIELDS

Important CPE Fields	
Field	***Example***
CPE Name	cpe:2.3:a:3com:3cserver:-:*:*:*:*:*:*:*
CPE ID	FFADC2E2-6888-490E-98CB-6D86D2E893A6
Last Modified	2011-01-12T14:35:43.867
Title	3Com 3CServer

E. Common Vulnerability Scoring System (CVSS)

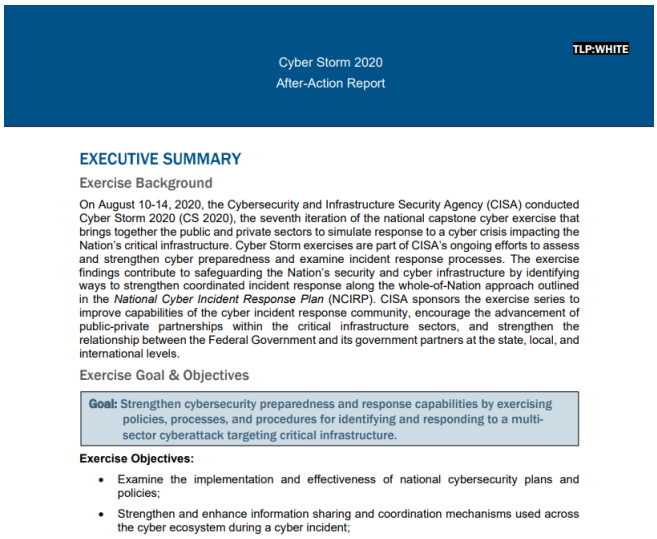
The Common Vulnerability Scoring System, or CVSS, is a standardized framework used to describe the severity of software vulnerabilities. The CVSS is owned and maintained by the non-profit organization FIRST.Org Inc[17]. The CVSS score is based on three metrics: Base, Temporal, and Environmental. The base score can be between 0 and 10. The score corresponds to an associated severity score: 0 is None, 0.1-3.9 is Low, 4.0-6.9 is Medium, 7.0-8.9 is High, and 9.0-10.0 is Critical. The National Institute of Standards and Technology, or NIST, has published a CVSS calculator[18] for CVEs on their website. CVSS scores can help cybersecurity experts prioritize which vulnerabilities to address first.

TABLE V
IMPORTANT CVSS FIELDS

Important CVSS Fields	
Field	***Example***
Vector String	CVSS:3.1/AV:N/AC:H/PR:L ...
Base Score	3.1(Low)
Temporal Score	3.0(Low)
Environment Score	3.0(Low)

F. After Action Reports (AARs)

Piplai et al [11] describe After Action Reports as being a good resource for extracting cyber attack information. AARs are created as unstructured text documents, and traditionally cyber analysts would need to read the documents to extract useful information manually. Figure V-F depicts an example AAR. Piplai et al [11] describe a system for extracting useful information from the reports using natural language processing (NLP) techniques and populating a knowledge graph with this information. Having these AARs in a structured format would allow researchers and analysts to find common attack patterns or trends automatically using intelligent tools.


Cyber Storm 2020
After-Action Report
TLP:WHITE

EXECUTIVE SUMMARY

Exercise Background

On August 10-14, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) conducted Cyber Storm 2020 (CS 2020), the seventh iteration of the national capstone cyber exercise that brings together the public and private sectors to simulate response to a cyber crisis impacting the Nation's critical infrastructure. Cyber Storm exercises are part of CISA's ongoing efforts to assess and strengthen cyber preparedness and examine incident response processes. The exercise findings contribute to safeguarding the Nation's security and cyber infrastructure by identifying ways to strengthen coordinated incident response along the whole-of-Nation approach outlined in the *National Cyber Incident Response Plan* (NCIRP). CISA sponsors the exercise series to improve capabilities of the cyber incident response community, encourage the advancement of public-private partnerships within the critical infrastructure sectors, and strengthen the relationship between the Federal Government and its government partners at the state, local, and international levels.

Exercise Goal & Objectives

Goal: Strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector cyberattack targeting critical infrastructure.

Exercise Objectives:

- Examine the implementation and effectiveness of national cybersecurity plans and policies;
- Strengthen and enhance information sharing and coordination mechanisms used across the cyber ecosystem during a cyber incident;

Fig. 3. An excerpt from an After Action Report [19].

VI. KNOWLEDGE GRAPH ONTOLOGY VISUALIZATION

We provide a visualization of the UCKG to help users dynamically explore, interact, and better understand the ontology and the UCKG. WebVOWL[19] is an open-source graphical user interface that provides this exact functionality. Classes are represented as labeled nodes in a graph connected by relationships. By clicking on various nodes and relationships, users will be shown detailed information about the selection including name, type, comments, and who defined the entity. Figure VI shows a screenshot from WebVOWL.

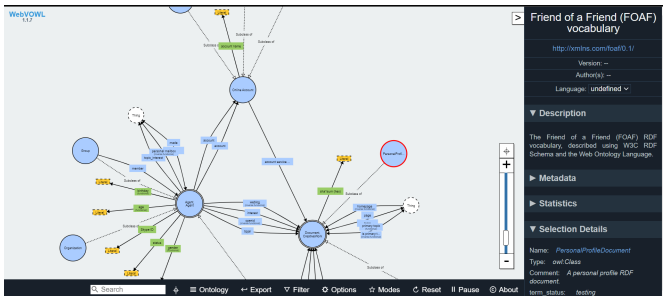


Fig. 4. Screenshot of WebVOWL user interface.

VII. INTELLIGENT CYBERSECURITY APPLICATIONS UTILIZING KNOWLEDGE GRAPHS

Various applications can be constructed that utilize an extensive knowledge graph containing platforms, weaknesses, and vulnerabilities. One major area is the study of attack flow,

[16]https://nvd.nist.gov/products/cpe
[17]https://www.first.org/cvss/
[18]https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
[19]http://vowl.visualdataweb.org/webvowl.html

how an attack develops and early recognition of the signs of an attack occurrence. Another possible application of an extensive cyber threat knowledge graph is the discovery of new vulnerabilities and threats. This includes the personalization of threat discovery specific to organizations with unique systems and cyber infrastructure. Log-based analysis as compared to an extensive knowledge base is another section of future study related to threat detection. Predicting Zero-Day attacks based on similar characteristics and patterns of current known cyber attacks could greatly benefit the general community of security professionals as well as offer an individual approach to preemptively protect company assets and data. Finally, an attack pattern knowledge graph can be used alongside intrusion detection systems to monitor traffic and predict live attacks that will happen or are currently in progress [2]. We intend to develop several use cases as future work to show the effectiveness of UCKG in real-world intelligent applications.

VIII. Conclusion and Future Work

In this paper, we presented UCKG, Unified Cybersecurity Knowledge Graph, a comprehensive KG towards collecting, integrating, unifying cybersecurity knowledge resources. The aim of UCKG is to provide a single point of reference for future intelligent cybersecurity applications. Our prototype application currently integrates data from open cybersecurity data resources such as CPE, CWE, CAPEC, CPE, and CVSS. UCO is the unifying vocabulary and ontology to unify integrated data sources and to build UCKG.

We plan to add AAR reports using NLP solutions and possibly Large Language Models (LLM). There is also high interest in mapping platform-specific logs, such as Microsoft SQL Server[20] logs in UCKG.

References

[1] Iannacone, M., Bohn, S., Nakamura, G., Gerth, J., Huffer, K., Bridges, R., Goodall, J. (2015, April). Developing an ontology for cyber security knowledge graphs. In Proceedings of the 10th Annual Cyber and Information Security Research Conference (pp. 1-4).

[2] Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., Zhou, Y. (2022). Recent progress of using knowledge graph for cybersecurity. Electronics, 11(15), 2287.

[3] Barnum, S. (2012). Standardizing cyber threat intelligence information with the structured threat information expression (STIX). Mitre Corporation, 11, 1-22.

[4] Guo, Y., Liu, Z., Huang, C., Wang, N., Min, H., Guo, W., Liu, J. (2023). A framework for threat intelligence extraction and fusion. Computers & Security, 132, 103371.

[5] Keshavarzi, M., Ghaffary, H. R. (2023). An ontology-driven framework for knowledge representation of digital extortion attacks. Computers in Human Behavior, 139, 107520.

[6] Qi, Y., Gu, Z., Li, A., Zhang, X., Shafiq, M., Mei, Y., Lin, K. (2023). Cybersecurity knowledge graph enabled attack chain detection for cyber-physical systems. Computers and Electrical Engineering, 108, 108660.

[7] Bryniarska, A., Pokuta, W. (2022). Ontology-Based Knowledge Representation in the IoT Cybersecurity System. Semantic Web Journal.

[8] Zhao, X., Jiang, R., Han, Y., Li, A., Peng, Z. (2023). A Survey on Cybersecurity Knowledge Graph Construction. Computers & Security, 103524.

[9] Syed, Z., Padia, A., Finin, T., Mathews, L., Joshi, A. (2016). UCO: A unified cybersecurity ontology. UMBC Student Collection.

[10] Sarker, I. H., Furhad, M. H., Nowrozy, R. (2021). AI-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2, 1-18.

[11] Piplai, A., Mittal, S., Joshi, A., Finin, T., Holt, J., Zak, R. (2020). "Creating cybersecurity knowledge graphs from malware after action reports." IEEE Access, 8, 211691-211703. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9264152

[12] Bolton, J., Elluri, L., Joshi, K. (2023). An Overview of Cybersecurity Knowledge Graphs Mapped to the MITRE ATT&CK Framework Domains. UMBC Center for Accelerated Real-Time Analysis.

[13] Sikos, L. F. (2023). Cybersecurity knowledge graphs. Knowledge and Information Systems, 1-21.

[14] Piplai, A. (2023). Knowledge Graphs and Reinforcement Learning: A Hybrid Approach for Cybersecurity Problems (Doctoral dissertation, University of Maryland, Baltimore County).

[15] Andrew, Y., Lim, C., Budiarto, E. (2023, August). Knowledge Graphs for Cybersecurity: A Framework for Honeypot Data Analysis. In 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs) (pp. 275-280). IEEE.

[16] Piplai, A., Kotal, A., Mohseni, S., Gaur, M., Mittal, S., & Joshi, A. (2023). Knowledge-enhanced Neuro-Symbolic AI for Cybersecurity and Privacy. arXiv preprint arXiv:2308.02031.

[17] Wang, P., Liu, J., Hou, D., & Zhou, S. (2022). A Cybersecurity Knowledge Graph Completion Method Based on Ensemble Learning and Adversarial Training. Applied Sciences, 12(24), 12947.

[18] Allemang, D., & Hendler, J. (2011). Semantic web for the working ontologist: effective modeling in RDFS and OWL. Elsevier.

[19] Cybersecurity and Infrastructure Security Agency. (2020). Cyber Storm 2020 After-Action Report. Retrieved from https://fsscc.org/wp-content/uploads/2021/02/Cyber_Storm-2020_After-Action-Report_01052021_Final.pdf

[20] Kiesling, E., Ekelhart, A., Kurniawan, K., & Ekaputra, F. (2019, October). The SEPSES knowledge graph: An integrated resource for cybersecurity. In International Semantic Web Conference (pp. 198-214). Cham: Springer International Publishing.

[21] Sharma, L. (2023, August 26). Knowledge Graph Construction with Ontologies in Neo4j— Part 2. Retrieved November 4, 2023, from Medium website: https://connect-lokesh.medium.com/knowledge-graph-construction-with-ontologies-in-neo4j-part-2-654f24da2a46

[20] https://www.microsoft.com/en-us/sql-server