Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence

Vasileios Mavroeidis
University of Oslo
Norway
vasileim@ifi.uio.no

Siri Bromander
mnemonic
University of Oslo
Norway
siri@mnemonic.no

***Abstract*—Cyber threat intelligence is the provision of evidence-based knowledge about existing or emerging threats. Benefits of threat intelligence include increased situational awareness and efficiency in security operations and improved prevention, detection, and response capabilities. To process, analyze, and correlate vast amounts of threat information and derive highly contextual intelligence that can be shared and consumed in meaningful times requires utilizing machine-understandable knowledge representation formats that embed the industry-required expressivity and are unambiguous. To a large extend, this is achieved by technologies like ontologies, interoperability schemas, and taxonomies. This research evaluates existing cyber-threat-intelligence-relevant ontologies, sharing standards, and taxonomies for the purpose of measuring their high-level conceptual expressivity with regards to the who, what, why, where, when, and how elements of an adversarial attack in addition to courses of action and technical indicators. The results confirmed that little emphasis has been given to developing a comprehensive cyber threat intelligence ontology with existing efforts not being thoroughly designed, non-interoperable and ambiguous, and lacking semantic reasoning capability.**[1]

***Index Terms*—threat intelligence, threat information sharing, cybersecurity, threat intelligence ontology, attribution, knowledge representation**

I. Introduction

Defenders utilize multiple diversified defense products to prevent, detect, and disrupt incoming attacks. However, the increasing capability, persistence, and complexity of adversarial attacks have made traditional defense approaches ineffective.

Organized cybercrime is at each peak. PwC's global economic crime survey of 2016 [1] reports that there are organizations that have suffered cybercrime losses over $5 million, and of these, nearly a third reported losses over $100 million. Juniper Research [2] reports that cybercrime will increase the cost of data breaches to $2.1 trillion globally by 2019, four times the estimated cost of breaches in 2015.

For enhancing their security posture, defenders recognized the need to understand threats their organization may face better and started exchanging threat information aiming one organization's detection to become another's prevention. This practice has achieved a certain maturity, with organizations focusing on generating and sharing more contextual and robust information known as cyber threat intelligence. Organizations rely on cyber threat intelligence to identify and understand impending attacks, speed up security operations, and drive and prioritize the implementation of security controls.

Threat intelligence is referred to as the task of gathering evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard[2]. Cyber threat intelligence needs to be relevant, timely, accurate, actionable, and contextual.

To a large extend, intelligence generation, consumption, and interpretation should be automated processes that leverage machine-understandable representation formats that allow for scalable processing, correlation, and analysis. A type of knowledge representation is ontologies. Ontologies encode knowledge about a particular domain in a structured manner, leverage logic for performing inference, and are flexible and modular, allowing them to be easily extended, refined, or interconnect with other ontologies.

Working towards an ontology for cyber threat intelligence has its challenges. Our research reports the following as the largest barriers to overcome:

- little focus on dedicated ontological cyber threat intelligence efforts that can account for the strategic, operational, and tactical levels;
- ambiguity in defined concepts that prevents ontology integration and adoption;
- extensive use of prose and limited utilization of existing taxonomies that undermine the querability of the knowledge base and minimize interoperability and the ability to perform reasoning;

[1]This paper is an updated version of DOI: 10.1109/EISIC.2017.20 and includes language enhancements. The changes in no case have affected the paper's scope, analysis, and derived conclusions. The original version of this research is included in the proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC).
Editor: Vasileios Mavroeidis
Date: February 2021

[2]https://www.gartner.com/doc/2487216/definition-threat-intelligence

- lack of relationships between concepts for augmented cyber threat intelligence interpretation and explainability;
- minimal use of ontology axioms and constructs that can be used for semantic consistency checking and information inference.

This article evaluates taxonomies, sharing standards, and ontologies relevant to the task of creating a comprehensive cyber threat intelligence ontology. To achieve that, we created the cyber threat intelligence model that indicates different types of information as abstraction layers that all together elucidate a malicious attack's five W's and one H; who, what, why, where, when, how, and technical indicators. We pinpoint the mappings between the cyber threat intelligence model and the taxonomies, sharing standards, and ontologies evaluated, aiming to indicate their expressivity. Finally, we critically review the shortcomings of the current cyber threat intelligence ontology approaches, and we discuss various directions to improving their quality.

II. Methodology

This section introduces two models related to threat detection maturity and cyber threat intelligence. The two models overlap, and both can meet different needs that are explained in the next two subsequent subsections. The Cyber Threat Intelligence model is the basis of the evaluation process conducted in this research.

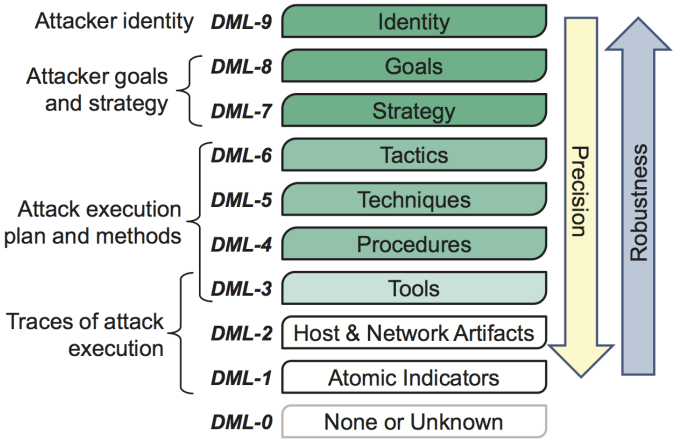

Fig. 1. Modified Detection Maturity Level Model [3] [4]

A. The Detection Maturity Level Model - DML

Ryan Stillions proposed the Detection Maturity Level (DML) model in 2014 [4]. DML is used to describe an organization's maturity regarding its ability to consume and act upon given cyber threat intelligence (Figure 1). Detection maturity at the higher levels of DML indicates that an organization has established intelligence-driven processes and procedures for detecting, understanding, and responding to cyber threats more effectively and efficiently. In 2016, we extended this model by adding an additional level (9) "Identity" and presented it for use in the semantic representation of cyber threats [3].

B. The Cyber Threat Intelligence Model

The Cyber Threat Intelligence model builds upon and extends [4] and [3], and intends to elucidate the different types of information an organization needs access to increase its situational awareness about threats. In this research, we utilize our model as a measurement standard. We use the model's distinguished cyber threat intelligence abstraction layers to measure the expressivity of existing taxonomies, sharing standards, and ontologies.

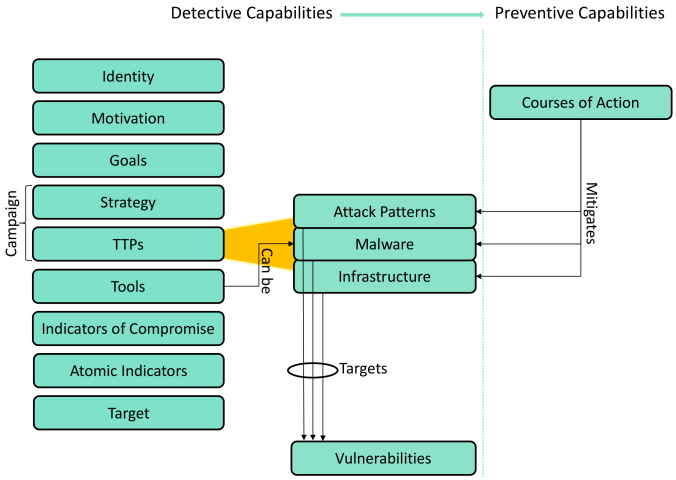

Fig. 2. Cyber Threat Intelligence Model

The remaining section is devoted to specifying the definitions of the elements comprising the cyber threat intelligence model.

Identity: the identity of a threat actor can be the real name of a person, an organization, a group's affiliates, or a nation-state-backed entity. In cases that attribution is not feasible, tracking operations via persona-based threat actor profiles also has its benefits as it allows identification of an actor's behavioral characteristics concerning their motivations, goals, capability, and TTPs they utilize.

Motivation: can be described as the driving force that enables actions to pursue specific goals. The goals of an attacker may change, but the motivation most of the times remains the same. Knowing a threat actor's motivation narrows down which targets that actor may focus on, helps defenders focus their limited defensive resources on the most likely attack scenarios, as well as shapes the intensity and the persistence of an attack [5]. Examples of motivation can be ideological, geopolitical, and financial.

Goals: according to Fishbach and Ferguson [6] "a goal is a cognitive representation of a desired endpoint that impacts evaluations, emotions, and behaviors". A goal consists of an overall end state and the behavior objects and plans needed for attaining it. The activation of a goal guides behaviors. Depending on how the attack is organized, the goal might not be known for the attacking team executing the attack. The team might only receive a strategy to follow. In current cyber threat intelligence approaches and knowledge bases goals are

mostly described in prose. A goal can be defined as a tuple of two: (Action, Object), but work needs to be done to create a consistent taxonomy at an adequate level of detail [3]. Typical examples of goals are "steal intellectual property", "damage infrastructure", and "embarrass a competitor".

Strategy: is a non-technical high-level description of the planned attack. There are typically multiple ways an attacker can achieve its goals, and the strategy defines which approach the threat agent should follow.

TTPs: tactics, techniques, and procedures are aimed to be consumed by a more technical audience. TTPs characterize adversary behavior in terms of what they want to achieve technically and how they are doing it.

Attack Pattern: is a type of TTP that describes behavior attackers use to carry out their attacks.

Malware: is a type of TTP and refers to a software that is inserted into a system with the intent of compromising the target in terms of confidentiality, integrity, or availability.

Infrastructure: describes any systems, software services, and any associated physical or virtual resources intended to support an adversarial operation, such as using purchased domains to support Command and Control, malware delivery sites, and phishing sites.

Tools: attackers install and use tools within the victim's network. Tools encompass both dedicated software developed for malicious reasons and software intended for different use (e.g., vulnerability and network scanning, remote process execution) but utilized for malicious purposes, mainly for avoiding detection (defense evasion).

Indicators of Compromise: are actionable technical elements and are directly consumable by cyber defense systems and components for detecting malicious or suspicious activity. A good IOC encompasses contextual information in addition to behavioral, computed, or atomic indicators to assist situational awareness.

Atomic Indicators: the value of atomic indicators is limited due to their short shelf life. Atomic indicators include file hashes, domain names, and IPs.

Target: represents the entity an attack is directed to and can be an organization, a sector, a nation, or individuals.

Course of Action: refers to measures that can be taken to prevent or respond to attacks.

C. Evaluation Criteria

Using open-source information such as published scientific works, documentation, and source files, the next section of the article presents and analyzes different taxonomies, sharing standards, and ontologies relevant to cyber threat intelligence. The conducted analysis/evaluation is based on the following criteria:

- Identify information and concepts covered in each work based on the abstraction layers of the Cyber Threat Intelligence model (Figure 2). Table 1 presents the results.
- Identify integrations (connections) between ontologies, taxonomies, and cyber threat intelligence sharing schemas for interoperability (Sections III, IV).
- Characterize the level of comprehensiveness and adequacy of semantic relationships in each work's conceptual layers and recognize the use of logics for information inference (Sections IV, V).

A number of identified articles present ontologies that are not described in great detail and have no reference to the actual ontology files (RDF/OWL), making their evaluation hard to achieve. Furthermore, some available ontology efforts do not offer an additional supporting publication and, most of the times, not even proper documentation.

III. Taxonomies and Sharing Standards

This section provides an overview of taxonomies and sharing standards that are used or potentially can be used in cyber threat intelligence representation. We categorize them as enumerations, scoring systems, and sharing standards.

A. Enumerations

TAL (Threat Agent Library) [7] is a set of standardized definitions and descriptions to represent significant threat agents. The library does not represent individual threat actors, thus it is not intended to identify people, or investigating actual security events. The goal of TAL is to help in risk management and specifically to identify threat agents relevant to specific assets. In that way, security professionals pro-actively can build defenses for specific threats.

Casey, in 2015, introduced a new taxonomy for cyberthreat motivations. The taxonomy identifies drivers that cause threat actors to commit illegal acts [5]. Knowing these drivers could indicate the nature of the expected harmful actions.

CVE (Common Vulnerabilities and Exposures) [8] is a list of records for publicly known information-security vulnerabilities in software packages.

NVD (National Vulnerability Database) [9] is a repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). The NVD performs analysis on CVEs that have been published to the CVE dictionary. This analysis results in association impact metrics (Common Vulnerability Scoring System - CVSS), vulnerability types (Common Weakness Enumeration - CWE), and applicability statements (Common Platform Enumeration - CPE), as well as other pertinent metadata. This data enables automation of vulnerability management, security measurement, and compliance.

CPE (Common Platform Enumeration) [10] is both a specification and a list. The specification defines standardized machine-readable methods for assigning and encoding names to IT product classes (software and hardware). The CPE dictionary provides an agreed-upon list of official CPE names.

CWE (Common Weakness Enumeration) [11] is a dictionary of software and hardware security weaknesses aiming to enhance understanding about common flaws and their mitigation.

CAPEC (Common Attack Patterns Enumerations and Characteristics) [12] provides a collection of the most common attack methods used to exploit known weaknesses.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) [13] is focused on network defense and describes the operational phases in an adversary's lifecycle, pre- and post-exploit, and details the TTPs adversaries use to achieve their objectives while targeting, compromising, and operating inside a network. It is a valuable resource to understand better adversary behavior and can be used for multiple purposes, such as for adversary emulation, behavioral analytics, cyber threat intelligence enrichment, defense gap assessment, and red teaming and SOC maturity assessment. ATT&CK matrices exist about adversary behavior targeting enterprise environments, mobile and industrial control systems. Moreover, information pertinent to software adversaries' use, mitigation techniques, procedure examples, and detection recommendations are also available.

B. Scoring Systems

CVSS (Common Vulnerability Scoring System) [14] is a measurement standard aiming to score vulnerabilities based on their severity. Combined with timely CTI, CVSS can inform an organization about which vulnerability remediation activities should prioritize.

CWSS (Common Weakness Scoring System) [15] is part of CWE and it provides a mechanism for scoring weaknesses using 18 different factors. It is worth mentioning that Mitre's Common Weakness Risk Analysis Framework (CWRAF) can be used in conjunction with CWSS to identify the most important CWEs applying to a particular business and their deployed technologies. The difference between CVSS and CWSS is that the first one targets specific software vulnerabilities scoring, whereas the latter one targets CWE scoring.

C. Sharing Standards

A study of existing threat intelligence sharing initiatives concluded that Structured Threat Information eXpression (STIX) is currently the most used standard for sharing threat information [16]. STIX is an expressive, flexible, and extensible representation language used to communicate an overall piece of threat information [17]. The STIX architecture comprises different cyber threat information elements such as cyber observables, indicators, incidents, adversaries tactics, techniques, procedures, exploit targets, courses of action, cyber attack campaigns, and threat actors. Furthermore, STIX was recently redesigned and as a result omits some of the objects and properties defined in the first version. The objects chosen for inclusion in the second version represent a minimally viable product that fulfills basic consumer and producer requirements for cyber threat intelligence sharing. Both standards can be used and adapted based on an organization's needs. It is worth pointing out that MITRE additionally offers MAEC (Malware Attribute Enumeration and Characterization) [18], a very expressive malware sharing language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns. MAEC can be integrated in STIX or used as a standalone.

OpenIOC, developed by Mandiant, is an extensible XML schema that enables you to describe the technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise. The types of information covered directly by OpenIOC are derived mainly by enriched low-level atomic indicators, comprising indicators of compromise, thus covering the IOC category of the cyber threat intelligence model.

IV. Ontologies

Since the work of Blanco et al. [19] in 2008, we have not found any overviews of existing ontologies within the cyber security domain. The authors remark that the scientific community has not accomplished a general security ontology because most of the works are focused on specific domains or the semantic web. The same conclusion was drawn by Fenz and Ekelhart [20]. Additionally, Blanco et al. [19] emphasize the complication of combining their identified ontologies due to the non-common interpretation and different terms applied to similar concepts in different ontologies. Our study confirms the same almost 10 years after the study of Blanco et al. [19].

While several ontologies relevant to the broader cybersecurity domain exist, only a small number was identified relating to threat information and threat intelligence representation. For a number of them, identifying the mappings to the abstraction layers of the cyber threat intelligence model is challenging because they are described only at a very high level and without having any relevant RDF/OWL files available for further investigation. The ontologies analyzed hereafter are listed chronologically based on their publication date.

Stefan Fenz and Andreas Ekelhat [20] described an information security ontology that can be used to support a broad range of information security risk management methodologies. The high-level concepts of the ontology are derived from the security relationship model described in the National Institute of Standards and Technology Special Publication 800-12. Concepts to represent the information security domain knowledge include threat, vulnerability, control, attribute, and rating. In addition, concepts such as asset, organization, and person are necessary to formally describe organizations and their assets. Lastly, the concept of location is integrated combined with a probability rating concept to interrelate location and threat information in order to assign priory threat probabilities. Like other works, the authors have difficulties connecting ambiguous concepts deriving from different standards (e.g., ambiguous distinction between a threat and a vulnerability).

Wang and Guo [21] proposed an ontology for vulnerability management and analysis (OVM) populated with all existing vulnerabilities in NVD. The basis of the ontology is built on the results of CVE and its related standards, such as CWE, CPE, CVSS, and CAPEC. OVM captures the relationships between the following concepts which constitute the top level of the ontology; vulnerability, introduction phase (software development life cycle - time periods during which the vulnerability can be introduced), active location (location of the software where the flaw manifests), IT product, IT

vendor, product category (such as web browsers, application servers, etc.), attack (integration of CAPEC), attack intent, attack method, attacker (human being or software agent), consequence, and countermeasure.

Obrst et al. [22] suggested a methodology for creating an ontology based on already well-defined ontologies that can be used as modular sub-ontologies. In addition, they remark the usefulness of existing schemas, dictionaries, glossaries, and standards as a form of knowledge acquisition of the domain by identifying and analyzing entities, relationships, properties, attributes, and range of values that can be used in defining an ontology. Their suggested ontology is based on the diamond model of malicious activity [23], which expresses the relationships between an adversary (actor), the capabilities of the adversary, the infrastructure or resources the adversary utilizes, and the target of the adversary (victim). The authors state that they developed first the aspects of infrastructure and capabilities, but they are still not in the level of detail they desire. In addition, their current ontology is focused on malware and some preliminary aspects of the diamond model.

A good argumentation for transitioning from taxonomies to ontologies for intrusion detection was made in 2003, by Undercoffer et al. [24]. They suggested an ontology that would enable distributed anomaly-based host IDS sensors to contribute to a common knowledge-base, which again would enable them to detect quicker a possible attack.

Based on this, More et al. [25] in 2012, suggested to build a knowledge-base with reasoning capabilities to take advantage of an extended variety of heterogeneous data sources, to be able to identify threats and vulnerabilities. Their data sources suggest that data retrieved and included in the ontology is within the atomic indicators category of the CTI model.

Oltramari et al. [26] proposed a three-layer cyber security ontology named "CRATELO" aiming at improving the situational awareness of security analysts, resulting in optimal operational decisions through semantic representation. Following the methodology of [22], the authors build upon existing ontologies and extend them. Specifically, CRATELO includes the top-level ontology DOLCE-SPRAY extended with security-related middle-level ontology (SECCO) capable of capturing details of domain specific scenarios, such as threat, vulnerability, attack, countermeasure, and asset. The low-level sub-ontology, cyber operations (OSCO), is the extension of the middle-level ontology.

Gregio et al. [27] suggested an ontology to address the detection of modern complex malware families whose infections involve sets of multiple exploit methods. To achieve this, they created a hierarchy of main behaviors each one of them consisting of a set of suspicious activities. Then they proposed an ontology that models the knowledge on malware behavior. They state that a given program behaves suspiciously if it presents one or more of the six events (main behaviors) described below which consist of several characteristics. The events are attack launching, evasion, remote control, self-defense, stealing, and subversion. When new set of process actions with malicious behaviors appear (input from "transformed" log files), the ontology can be inferred to see if an instance of suspicious execution is linked to a malware sample.

Salem and Wacek [28] designed a data extraction tool called TAPIO (Targeted Attack Premonition using Integrated Operational data), specializing in extracting data (through the use of natural language processing) and automatically mapping that data into a fully linked semantic graph accessible in real-time. Part of TAPIO is a cybersecurity ontology known as Integrated Cyber Analysis System (ICAS) that ingests extracted data (logs and events) from several sources to provide relationships across an enterprise network. The tool aims to help incident response teams connect and correlate events and actions into an ontology for automatic interpretation. ICAS is a collection of 30 sub-ontologies specializing in specific conceptual areas as part of host-based and network-based conceptual models.

Iannacone et al. [29] described their STUCCO ontology, which is developed to work on top of a knowledge graph database. The STUCCO ontology design is based upon scenarios of use by both human and automated users and incorporates data from 13 different structured data sources with different format. The data included in the current STUCCO ontology fall into the categories identity, TTPs, tools, and atomic indicators of our cyber threat intelligence model. Their future work included extending the ontology to support STIX.

Gregio, Bonacin, de Marchi, Nabuco, and de Geus [30] extended the work of Gregio et al. [27] and introduced the malicious behavior ontology (MBO). MBO is capable of detecting modern complex malware families whose infections involve sets of multiple exploit methods, by applying SWRL rules to the ontology for inferencing. In addition, these rules also apply metrics to specify whether a program is behaving maliciously or not and specifically, how suspicious the execution of a program is. The authors state that their model is able to detect unknown malicious programs even in cases where traditional security mechanisms like antivirus are not, by performing automatic inference of suspicious executions in monitored target systems. However, the current state of the ontology has some limitations such as performance issues, cannot detect malware in real time, and false positives and negatives. Based on its operation MBO can provide useful indicators of compromise for malware.

Fusun et al. suggested ontologies like attacks, systems, defenses, missions, and metrics for quantifying attack surfaces [31]. Their Attack Surface Reasoning (ASR) gives a cyber defender the possibility to explore trade-offs between cost and security when deciding on their cyber defense composition. ASR is mainly modeled after the Microsoft STRIDE [32] threat classification framework, which categorizes attack steps into 6 categories and is to the extent of our knowledge not the preferred framework within threat intelligence community due to its lack of details. In comparison, CAPEC and CPE have around 500 and 1000 categories, respectively.

As part of their study on using security metrics for security modeling, Pendelton et al. suggested the Security Metric Ontology [33]. The ontology includes four sub-ontologies; vulnerability, attack, situations and defense mechanisms, and

describes the relationship between them. The terminology used is somewhat different than that of known taxonomies, and their aim at modeling metrics is more prominent than that of analysis and reasoning. The ontology is published on GitHub[3].

The Unified Cybersecurity Ontology was suggested by Syed et al. [34] in 2016. It serves as a backbone for linking cyber security and other relevant ontologies. There are mappings to aspects of STIX, and references to CVE, CCE, CVSS, CAPEC, STUCCO and KillChain. The concepts are loosely connected at a very high level and the lack of OWL constructs decreases the reasoning capabilities of the ontology. In addition, our analysis indicate that the use of domain and range restrictions would result in faulty classifications when used with a reasoner. The ontology is published on GitHub[4].

The Unified Cyber Ontology has been introduced on GitHub[5], without any academic publications to date and no actual RDF/OWL files yet. The model ontology is however interesting as it originates from the creators of STIX, which is currently the most used format for sharing threat intelligence [16]. The content of that work is driven primarily by the initial base requirements of expressing cyber investigation information and is the product of input from the Cyber-investigation Analysis Standard Expression community (CASE)[6].

Without any publication, we find the Cyber Intelligence Ontology (CIO), published only on GitHub[7] to be relevant. This GitHub repository includes most of the mentioned taxonomies and sharing standards in this article, encoded in OWL. The limitation of those ontologies is that they are not connected or unified. For the aforementioned reason, we do not include CIO in the analysis and the evaluation table.

V. Discussion

Intelligence-driven defense augments organizations' detecting and responding capabilities and introduces a more informed preventive approach to the overall cybersecurity operations. The maturity, the analytical skills, and the available information sources of a security team determine their capability to produce accurate and actionable threat intelligence [35] [36].

To leverage the benefits of ontologies and description logics in cyber threat intelligence, we need unambiguous representations with sufficient expressivity and robust explicable bindings between concepts. A reference architecture like the one provided by our Cyber Threat Intelligence model can be used as an engineering blueprint that can support the fundamental development of concepts through modular domain ontologies that can be the basis for establishing a bigger and more comprehensive ontology that is extensible and adaptive. The analysis of the existing ontological efforts confirmed that there is still a small focus and much work to be done to establish a comprehensive and unambiguous cyber threat intelligence ontology.

Ontologies are modular and extensible, allowing replacing or integrating with other domain-focused ontologies to build a more holistic one that can benefit from an augmented representation regarding a domain of interest. In the ontologies evaluated, we identified that the lack of OWL expressions is a common phenomenon. Expressions make ontologies powerful by encoding domain expertise for reasoning. Using the encoded knowledge, a reasoner can infer new information from the existing asserted information at machine speed, introducing a form of automation.

Furthermore, we cannot ignore mentioning the limited taxonomy encodings and integrations we observed and the missing interconnections between those taxonomies and existing ontologies for establishing more standardized (interoperability) and expressive representations that resolve ambiguity, like taxonomies that standardize threat actor motivations, goals, and types. The importance of standardizing and utilizing taxonomies is apparent in cases where higher querability levels are desired.

Overall, an ontology gives access to a knowledge base containing rich historical and present information in a robust, meaningful, and explicable way. Analysts can utilize a cyber threat intelligence ontology to perform analytical tasks while decreasing the confirmation biases entailed in purely manual analytical and decision-making processes.

VI. Conclusion

Our study concluded that there is much work to achieve before establishing a contextual and unambiguous cyber threat intelligence ontology. Barriers to overcome include little focus on dedicated ontological cyber threat intelligence efforts that can account for the strategic, operational, and tactical levels; ambiguity in defined concepts that prevents ontology integration and adoption; extensive use of prose and limited utilization of existing taxonomies that undermine the querability of the knowledge base and the ability to perform reasoning; lack of relationships between concepts that can support interpretation and explainability; and minimal use of ontology axioms and constructs that can be used for semantic consistency checking and information inference.

[3]https://github.com/marcusp46/security-metrics-ontology
[4]https://github.com/Ebiquity/Unified-Cybersecurity-Ontology
[5]https://github.com/ucoProject/uco
[6]https://github.com/casework/case
[7]https://github.com/daedafusion/cyber-ontology

TABLE I
EVALUATION OF TAXONOMIES, SHARING STANDARDS, AND ONTOLOGIES

		Identity	Motivation	Goal	Strategy	TTP	Tool	IOC	Atomic Indicator	Target	COA
Taxonomies	TAL [7]	*									
	Threat Agent Motivation [5]	*	*								
	CVE [8]								*		
	NVD [9]								*		
	CPE [10]								*		
	CWE [11]					*			*		*
	CAPEC [12]					*		*			*
	ATT&CK [13]	*				*	*				
	CVSS [14]								*		
	CWSS [15]								*		
Sharing Standards	STIX 1 [17]	*	*	* (Intended Effect:taxonomy)	*	*	*	*	*	*	*
	STIX 2 [37]	*	*	* (Objectives:string)	*	*	*	*	*	*	*
	MAEC [18]							*			
	OpenIOC [38]					*	*	*	*		
Ontologies	Fenz & Ekelhat (2009) [20]								*		
	Wang & Guo (2009) - OVM [21]					*			*		*
	Orbst et al. (2012) [22]	*					*		*	*	
	More et al. (2012) [25]					*			*		
	Oltramari et al. (2014) - CRATELO [26]	*				*			*	*	
	Gregio et al. (2014) [27]						* (malware)		*		
	Salem & Wacek (2015) - ICAS [28]					*			*		
	Iannacone et al. (2015) - STUCCO [29]	*				*	*		*		
	Gregio et al. (2016) - MBO [30]						* (malware)	*	* (it may provide)		
	Fusun et al. (2015) - ASR [31]					*			*	*	
	Pendelton et al. (2016) - Security Metrics Ontology [33]					*					*
	Syed et al. (2016) - UCO [34]	*	*	*	*	*	*	*	*		*
	Unified Cyber Ontology (2016) - UCO [39]	*	*	*	*	*	*	*	*	*	*

REFERENCES

[1] K. McConkey, "Cybercrime: A Boundless Threat," https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html.

[2] S. Smith, "Cybercrime will Cost Businesses over $2 Trillion by 2019," https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

[3] S. Bromander, A. Jøsang, and M. Eian, "Semantic Cyberthreat Modelling," in *STIDS*, 2016, pp. 74–78.

[4] R. Stillions, "The DML Model," http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html.

[5] T. Casey, "Understanding cyber threat motivations to improve defense," *Intel White Paper*, 2015.

[6] A. Fishbach and M. J. Ferguson, "The goal construct in social psychology." 2007.

[7] T. Casey , "Threat Agent Library Helps Identify Information Security Risks," *Intel White Paper, September*, 2007.

[8] MITRE, "Common Vulnerabilities and Exposures," https://cve.mitre.org.

[9] NIST, "National Vulnerability Database," https://nvd.nist.gov/.

[10] Mitre, "Common Platform Enumeration," https://cpe.mitre.org/specification/.

[11] MITRE, "Common Weakness Enumeration," https://cwe.mitre.org.

[12] MITRE, "Common Attack Pattern Enumeration and Classification," https://capec.mitre.org/.

[13] MITRE, "Adversarial Tactics, Techniques and Common Knowledge," https://attack.mitre.org/.

[14] NIST, "Common Vulnerability Scoring System," https://nvd.nist.gov/vuln-metrics/cvss.

[15] MITRE, "Common Weakness Scoring System," https://cwe.mitre.org/cwss/cwss_v1.0.1.html.

[16] C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives," 2017.

[17] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX ™)," *MITRE Corporation*, vol. 11, 2012.

[18] Mitre, "Malware Attribute Enumeration and Characterization," https://maec.mitre.org.

[19] C. Blanco, J. Lasheras, R. Valencia-García, E. Fernández-Medina, A. Toval, and M. Piattini, "A Systematic Review and Comparison of Security Ontologies," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*. Ieee, 2008, pp. 813–820.

[20] S. Fenz and A. Ekelhart, "Formalizing Information Security Knowledge," in *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*. ACM, 2009, pp. 183–194.

[21] J. A. Wang and M. Guo, "OVM: An Ontology for Vulnerability Management," in *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*. ACM, 2009, p. 34.

[22] L. Obrst, P. Chase, and R. Markeloff, "Developing an Ontology of the Cyber Security Domain," in *STIDS*, 2012, pp. 49–56.

[23] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," DTIC Document, Tech. Rep., 2013.

[24] J. Undercoffer, A. Joshi, and J. Pinkston, "Modeling Computer Attacks: An Ontology for Intrusion Detection," in *International Workshop on Recent Advances in Intrusion Detection*. Springer, 2003, pp. 113–135.

[25] S. More, M. Matthews, A. Joshi, and T. Finin, "A Knowledge-Based Approach to Intrusion Detection Modeling," in *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on*. IEEE, 2012, pp. 75–81.

[26] A. Oltramari, L. F. Cranor, R. J. Walls, and P. D. McDaniel, "Building an Ontology of Cyber Security," in *STIDS*. Citeseer, 2014, pp. 54–61.

[27] A. Grégio, R. Bonacin, O. Nabuco, V. M. Afonso, P. L. De Geus, and M. Jino, "Ontology for Malware Behavior: a Core Model Proposal," in *WETICE Conference (WETICE), 2014 IEEE 23rd International*. IEEE, 2014, pp. 453–458.

[28] M. B. Salem and C. Wacek, "Enabling New Technologies for Cyber Security Defense with the ICAS Cyber Security Ontology," in *STIDS*, 2015, pp. 42–49.

[29] 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," in *Proceedings of the 10th Annual Cyber and Information Security Research Conference*. ACM, 2015, p. 12.

[30] A. Grégio, R. Bonacin, A. C. de Marchi, O. F. Nabuco, and P. L. de Geus, "An Ontology of Suspicious Software Behavior," *Applied Ontology*, vol. 11, no. 1, pp. 29–49, 2016.

[31] M. B. Fusun, A. S. Yaman, T. Marco, E. Carvalho, and C. N. Paltzer, "Using Ontologies to Quantify Attack Surfaces."

[32] A. Shostack, *Threat Modeling: Designing for Security*. John Wiley & Sons, 2014.

[33] M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu, "A Survey on Systems Security Metrics," *ACM Computing Surveys (CSUR)*, vol. 49, no. 4, p. 62, 2016.

[34] Z. Syed, A. Padia, M. L. Mathews, T. Finin, and A. Joshi, "UCO: A Unified Cybersecurity Ontology," in *Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security*. AAAI Press, 2016.

[35] T. Rid and B. Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, vol. 38, no. 1-2, pp. 4–37, 2015.

[36] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," *NIST Special Publication*, vol. 800, p. 150, 2016.

[37] OASIS CTI TC, "Structured Threat Information Expression (STIX ™) 2.0," https://oasis-open.github.io/cti-documentation/, 2017.

[38] Mandiant Corporation, "Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC," http://www.openioc.org/resources/An_Introduction_to_OpenIOC.pdf, 2013.

[39] "Unified Cyber Ontology," https://github.com/ucoProject/uco, 2016.