Using Semantic-Web Technologies for Situation Assessments of Ethical Hacking High-Value Targets

Sanjana Suresh, Rachel Fisher, Radha Patole, Andrew Zeyher and Thomas Heverin
Drexel University, USA
ss5264@drexel.edu
rcf49@drexel.edu
rdp74@drexel.edu
az458@drexel.edu
th424@drexel.edu

DOI: 10.34190/EWS.21.070

Abstract: Ethical hacking consists of scanning for targets, evaluating the targets, gaining access, maintaining access, and clearing tracks. The evaluation of targets represents a complex task due to the number of IP addresses, domain names, open ports, vulnerabilities, and exploits that must be examined. Ethical hackers synthesize data from various hacking tools to determine targets that are of high value and that are highly susceptible to cyber-attacks. These tasks represent situation assessment tasks. Previous research considers situation assessment tasks to be tasks that involve viewing an initial set of information about a problem and subsequently piecing together more information to solve the problem. Our research used semantic-web technologies, including ontologies, natural language processing (NLP), and semantic queries, to automate the situation assessment tasks conducted by ethical hackers when evaluating targets. More specifically, our research focused on automatically identifying education organizations that use industrial control system protocols which in turn have highly exploitable vulnerabilities and known exploits. We used semantic-web technologies to reduce an initial dataset of 126,636 potential targets to 155 distinct targets with these characteristics. Our research adds to previous research on situation assessment by showing how semantic-web technologies can be used to reduce the complexity of situation assessment tasks.

Keywords: ontology modeling, situation assessment, target evaluation

1. Introduction

Ethical hacking consists of several phases including identifying targets, evaluating targets, gaining access, maintaining access, and clearing tracks. Evaluating targets consists of finding information about organizations such as IP addresses, hardware names/versions, software names/versions, ports, protocols, and services (Morris and Gao, 2013). For evaluating targets, ethical hackers also research vulnerabilities connected to the aforementioned information as well as exploits that can be used on the vulnerabilities.

Target evaluation often starts with finding targets based on the type of organization (organization-type) and the types of assets an organization holds (asset-type). High-value organization-types include organizations that, if attacked, could result in severe consequences for individuals, organizations, and communities. Examples of high-value organization-types include organizations that are identified as “critical infrastructure” organizations. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), there are 16 critical infrastructure sectors that are so vital that “...their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof” (CISA, 2020). Table 1 shows the 16 critical infrastructure sectors according to CISA.

Table 1: Critical infrastructure sectors According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA)

Chemical Sector	Commercial Facilities Sector	Communications Sector	Critical Manufacturing Sector
Dams Sector	Defense Industrial Base Sector	Emergency Services Sector	Energy Sector
Financial Services Sector	Food and Agriculture Sector	Government Facilities Sector	Healthcare and Public Health Sector
Information Technology Sector	Nuclear Reactors, Materials, and Waste Sector	Transportation Systems Sector	Water and Wastewater Systems Sector

In addition to ethical hackers identifying high-value targets based on organization-types, ethical hackers also select targets based off of asset-types. High-value asset-types across organizations include industrial control systems (ICS). ICS are systems that control the physical operation of entities such as electrical systems, building automation systems, physical security systems, ventilation systems, military weapon systems, ship systems and more. ICS are found across all types of sectors including education, government, manufacturing, military, commercial, and electrical power. An attack on ICS could cause wide-spread electrical outages, disrupt everyday work activities, cause organizations to stop production, cause physical harm to people, and compromise safety (Morris and Gao, 2013).

Furthermore, highly exploitable ICS devices are considered to be even more valuable targets for ethical hackers. These types of devices are considered to have easy-to-exploit vulnerabilities which in turn have publicly known exploits. Many ICS protocols were originally designed without security in mind, resulting in a high level of risk for ICS. Vulnerabilities of ICS protocols include the lack of integrity, confidentiality, availability, authentication, authorization, and encryption. There are many types of cyber-attacks that can exploit these vulnerabilities such as denial-of-service, data injection, and command injection attacks (Morris and Gao, 2013).

Based on this information, an individual can reason that highly exploitable ICS devices (high-value asset-types) found within critical infrastructure organizations (high-value organization-types) are prime targets for ethical hackers. For this research paper, our focal point consisted of education organizations which fall under the "Government Facilities Sector" critical infrastructure category (CISA, 2020). Education targets include kindergarten through grade 12 (K-12) schools, institutions of higher education, and business and trade schools.

K-12 remote learning has suffered from a multitude of cyber-attacks. According to the U.S. Federal Bureau of Investigation (FBI), CISA, and the Multi-State Information Sharing and Analysis Center (MS-ISAC), K-12 schools are increasingly targeted by malicious cyber-attackers, "leading to ransomware attacks, the theft of data, and the disruption of distance learning services" (FBI, CISA, and MS-ISAC, 2020). These cyber-attacks are expected to continue throughout the course of remote learning and cause grave issues for K-12 schools due to their limited resources. Alongside K-12 schools, colleges and universities have increasingly become targets because of their new technology development, innovation, and research activities (Rogers and Ashford, 2015). Our research aims to reduce the complexity of target evaluation, a situation assessment task, in the education sector. The results of our research can contribute to better protecting K-12 schools, colleges, and universities.

2. Background

The goal of our research was to explore how we can automate the target evaluation phase of ethical hacking. In this section, we thread together research on situation assessment and ontologies in the cybersecurity domain.

2.1 Situation assessment

Situation assessment represents an information-intensive task that involves finding an initial set of information about a problem, evaluating information, finding more information, and integrating new information into existing evidence (Ben-Bassat and Freedy, 1982; Gorodetsky et al., 2005). Situation assessment also involves clarifying a problem and developing a plan to solve that problem (Kirillov, 1994; Noble, 1993; Salas et al., 2010). Once situation assessment is complete, it leads to obtaining situation awareness (Endsley and Garland, 2000). The process of forming a situation assessment is called completing a "situation assessment task" (Noble et al., 1986). Ben-Bassat and Freedy (1982, p. 489) consider a situation assessment task to be a "puzzle building task", as problem solvers synthesize information to understand a situation.

Previous research has shown that decision makers complete situation assessment tasks based on mental schemas that have been developed over years of experience. Lipshitz and Shaul (1997, p. 295) define schema as "situation or domain specific cognitive structures that (a) direct external information search, (b) specify which available information will be attended to and which information will be ignored, (c) organize information in memory, (d) direct the retrieval of information from memory, and (e) become more differentiated as a function of experience." Schemas provide a way for people to determine what information needs to be found, how to find the information, and how to piece the information together to make decisions (Lipshitz and Shaul, 1997; Noble et al., 1986; Serfaty et al., 1997). According to Elliot (2005, p. 215), "A schema helps determine what we attend to, what we perceive, and what we remember and infer."

In terms of the target evaluation phase of ethical hacking, situation assessment tasks involve the use of various resources to piece together information to select exploitable targets. This information includes organization names and types, IP addresses, open ports, protocols in use, software in use, vulnerability information, exploit information, and more. Even though ethical hacking and other cybersecurity domains, such as cyber forensics, consist of situation assessment tasks, only limited research on situation assessment in the cybersecurity domain exists.

Research has been conducted on determining how cyber defenders, those who protect networks against cyber-attacks, synthesize various pieces of information to detect and analyze cyber-attacks (Barford et al., 2010; D’Amico et al., 2005). Cyber defenders must sift through multiple sources, such as network logs, email logs, server logs, computer logs and more, to determine if a cyber-attack is taking place and to understand what an attack is doing. Cyber defenders also use online sources to find information. These sources include the National Vulnerability Database (NVD), VirusTotal, Wireshark, U.S. Computer Emergency Readiness Team (CERT), and more.

Cyber defenders then fuse the data that they collect from multiple sources to determine what steps they need to take to contain and eradicate cyber-attacks on their networks (D’Amico et al., 2005; Goodall et al., 2009). The deluge of data that must be reviewed can cause an information overload for cyber defenders (D’Amico et al., 2005; Tyworth et al., 2012; Yen et al., 2010).

Although some research using ontologies to model domains within cybersecurity exists, there is a lack of research on how semantic-web technologies can be used to aid situation assessment tasks in the ethical hacking domain.

2.2 Ontologies and cybersecurity

Ontologies are used to specify a domain, its entities, and the relationships among those entities (World Wide Web Consortium, 2015). Ontologies often provide the foundation of artificial intelligence (AI) systems. As Gruber stated (1993, p. 1), “To support the sharing and reuse of formally represented knowledge among AI systems, it is useful to define the common vocabulary in which shared knowledge is represented. A specification of a representational vocabulary for a shared domain of discourse — definitions of classes, relations, functions, and other objects — is called an ontology.” An ontology is also often described as a web of data or a “semantic-web.”

Ontologies are primarily made up of classes (categories of objects), objects that fall in those classes, object properties that link classes (as well as objects) with each other, and data properties that contain metadata about the objects. Resource description framework (RDF) is used as a standardized framework to describe all these ontology concepts (World Wide Web Consortium, 2015). After a domain is modeled with an ontology, one can run queries over the ontology to find new relationships and to discover new knowledge.

Queries over ontologies can help make decisions and form plans. As Gruber stated (1993, p. 3), a query system over an ontology “...takes descriptions of objects, events, resources, and constraints, and produces plans that assign resources and times to objects and events.” The queries take inputs from an ontology and produce outputs to allow planners to perform their tasks. In terms of ethical hacking, an ontology could be used to ingest reconnaissance and scanning information to identify high-value targets which will allow ethical hackers to complete their tasks. Various semantic-web technologies can be used to query or search across a web of data. SPARQL, a recursive acronym for SPARQL query language, is a standard query language used for ontologies.

Previous research has focused on using ontologies for various reasons in cybersecurity. Grant, van’t Wout, and van Niekerk (2020) created an ontology to assist with intelligence, surveillance, target acquisition and reconnaissance. Falk (2016) showed how ontologies can be used to organize open-source threat intelligence sources in order to build a comprehensive view of a threat environment. Aviad, Wecel and Abroamowicz (2015) focused on using ontologies to link known attacks with information technology (IT) products to develop a cybersecurity body of knowledge. Their research aimed to provide threats based off of a given configuration. Other research has focused on expanding the cybersecurity body of knowledge (Takahashi and Kadobayashi, 2015), creating an ontology that links together log and forensics data (Balduccini, Kushner, and Speck, 2015), and developing a taxonomy of ICS with an ontology (Flowers, Smith, and Oltramari, 2016). There lacks research on using an ontology for target evaluation.

3. ICS target ontology

In this section, we describe the structure of our ontology, called the ICS Target Ontology, and methods used to fill the ontology with relevant data to help with target evaluation.

3.1 Ontology structure

In an ontology, classes represent categories of objects. An example class in the ICS Target Ontology is "ICS Protocol." Representative objects in this class include popular ICS protocols such as BACnet, Modbus, S7, and Ethernet/IP. Another example class is "IP Address" which is filled with specific IP addresses. Other classes in the ontology include "Organization", "Port Number", "Vulnerability", and "Exploit."

Object properties are used to define relationships between classes; objects properties are then specified (filled out) to show specific links between two named objects. An example of an object property in the ICS Target Ontology is *usesProtocol* which defines a relationship between the classes IPAddress and ICS Protocol. We can say that IPAddress *usesProtocol* ICS Protocol. A specification of this object property is 123.45.67.89 *usesProtocol* BACnet.

The key object properties in the ICS Target Ontology are shown below in Table 2. A domain is the "subject" of an object property while the Range is the object of the object property.

Table 2: Object properties found in the ICS target ontology

Domain	Object Property	Range
Organization	*usesIPAddress*	IPAddress
IPAddress	*usesPort*	PortNumber
PortNumber	*usesProtocol*	ICSProtocol
ICSProtocol	*hasVulnerability*	Vulnerability
Vulnerability	*isExploitedBy*	Exploit

Within an ontology, a data property is used to define metadata about an object. An example data property includes "OrganizationType", and for this data property we can state values such as "Education", "Government", "Manufacturing", and more. A specification of this data property is: the data property value for the OrganizationType associated with Drexel University is Education.

The data properties in the ICS Target Ontology, their associated classes, and their possible values are shown below in Table 3.

Table 3: Data properties found in ICS target ontology

Data Property Name	Class	Possible Values
AttackComplexity	Vulnerability	Low or High
AttackVector	Vulnerability	Physical, Local, Adjacent Network or Network
AvailabilityImpact	Vulnerability	None, Low or High
ConfidentialityImpact	Vulnerability	None, Low or High
CVSS_BaseScore	Vulnerability	Numeric Score (out of 10)
ExploitabilitySubscore	Vulnerability	Numeric Score (out of 3.9)
ImpactSubscore	Vulnerability	Numeric Score (out of 6.0)
IntegrityImpact	Vulnerability	None, Low or High
OrganizationTargetValue	Organization	Low, Medium or High
OrganizationType	Organization	Education, IT, Communications, Food, Government, and More
PrivilegesRequired	Vulnerability	None, Low or High
UserInteraction	Vulnerability	None or Required

The vulnerability data properties are drawn from the NVD Common Vulnerability Scoring System Calculator (CVSS). The OrganizationType data property was derived from the critical infrastructure categories shown in Table 1.

The "OrganizationTargetValue" data property was derived from Factor Analysis of Information Risk (FAIR) which represents a model of risk factors and the relationships between the factors (Freund and Jones, 2014). As a standard quantitative model, FAIR serves as a widely accepted measure of assessing risks and cyberthreats. FAIR is comprised of two major categories: threats and assets. In the education sector, if a threat caused a denial-of-service, the threat could significantly disrupt education organizations from providing education services and protecting the safety of the populations they serve. Therefore, education organizations were deemed to have an OrganizationTargetValue of "high."

3.2 Data processing

Our ontology was created using Protégé, an open-source ontology editor. The classes, object properties, and data properties created "slots" for data ingestion. To find potential education organizations that use ICS protocols, we created searches in Shodan, an open-source search engine for Internet-connected devices. The searches focused on popular ICS protocols including BACnet, Modbus, S7 and Ethernet/IP. These searches generated over 126,000 publicly available ICS targets which are shown in Table 4 below. The Shodan data were then exported to a comma-separated values (CSV) file for further data processing.

Table 4: ICS protocol search results from Shodan

ICS Protocol/Port	Description of ICS Protocol	Number of IP Addresses from Shodan for ICS Protocols
BACnet/47808 (UDP)	Building automation systems protocol	21,136
Modbus/502 (TCP)	Popular protocol for ICS	14,523
S7/102 (TCP)	Siemens ICS protocol for programmable logic controllers (PLCs)	36,039
Ethernet IP/44818 (UDP)	Industrial Ethernet network protocol	54,938
	Total	126,636

The exported Shodan CSV file consisted of various data fields including organization name, IP address, ports, domain names, and more. The "organization name" data field provided an opportunity to determine how to identify organizations such as education organizations.

Two researchers manually examined a set of 1,500 entries from the Shodan CSV file to identify education organizations. There was a 99% agreement rate between the two researchers' identification of education organizations.

We then used the Natural Language Toolkit (NLTK), which contains Python libraries and programs for statistical NLP, to determine how to automate the identification of education organizations. NLTK was used on the initial dataset (1,500 entries) that was manually examined. The initial success rate for identifying education organizations was 98.1% overall. At first, NLTK incorrectly identified organizations that had "universal" in their names as education organizations. We tweaked the NLTK libraries and then found a success rate of 100% based on the initial 1,500 entries.

From there, we used NLTK to analyze key words from each education organization name from the initial data set (such as "university", "school", "college", and these terms in multiple languages) and used the Python library called "Wordnet" to build a list of synonyms. The list of synonyms was then used in NLTK to identify additional organizations that were not included in the initial dataset. For example, in the initial dataset, there were no entries that had "education" in the organization names. Wordnet generated "education" as a synonym for "school" which then allowed NLTK to identify entities like "Philadelphia Education Network" as an education organization. As another example, "higher education" was generated as a synonym for the terms "university" and "college."

With the Wordnet synonym list, we ran NLTK over the Shodan CSV file of 126,636 entries. NLTK identified 2,272 education targets in 2.12 seconds and created a value for "Education" for Organization Type in the CSV file. Two researchers manually reviewed 500 targets of the NLTK CSV file and found agreement across all entries.

We used a utility within Protégé called "Create Axioms from Excel Workbook" that provides methods for ingesting data from CSV files into an ontology and linking data from the CSV files to ontology classes, object properties and data properties. For example, common vulnerabilities and exposures (CVEs) and their data properties were already in the ICS Target Ontology. Protégé allowed us to link targets directly to the CVEs upon importing the Shodan data.

Although 2,272 targets represent a considerably smaller number than 126,636 targets, a list of 2,272 targets still produces a complex situation assessment task in determining which targets are highly exploitable. Semantic queries, described in the next section, provide a method for finding targets that are highly exploitable.

4. Target evaluation query and results

4.1 SPARQL

While ontologies are used to model a domain, semantic queries are used to provide answers to questions about a domain. SPARQL is a set of specifications that provide languages and protocols to query ontologies (World Wide Web Consortium, 2013). SPARQL can be used to design simple queries (such as listing data property values for a specific object) and complex queries (such as determining the shortest path, among multiple paths, from one object to another object that is 100 objects away) (Angle and Guiterrez, 2008).

Types of queries available in SPARQL include union, filters, value aggregation, nested queries and more. SPARQL queries produce outputs, often in the form of tables, and can include solution modifiers such as distinct, order, and limit modifiers. Also, "...the output of a SPARQL query can be of different types: yes/no queries, selections of values of the variables which match the patterns, construction of new triples from these values, and descriptions of resources" (Pérez, J., Arenas, M., & Gutierrez, 2006, p. 30). As a result, SPARQL queries can be used to aid in situation assessment tasks completed by ethical hackers such as finding high-value targets that have highly exploitable vulnerabilities over a specific port number.

4.2 SPARQL complex query for target evaluation

Various queries were developed to assist with the situation assessment task of finding high-value targets that use ICS protocols which in turn have highly exploitable vulnerabilities and known exploits. We examined several types of queries focused on various object properties and data properties. After testing several queries and reviewing the query outputs, we developed a complex query focused on the following parameters:

- Target with "OrganizationType" value of *Education*
- Target with "Target Value" value of *High*
- Target that uses an ICS protocol via the object property *usesProtocol*
- Vulnerability with "Attack Complexity" value of *Low* (easy to attack)
- Vulnerability with "Attack Vector" value of *Network* (remotely exploitable)
- Vulnerability with "Privileges Required" value of *None* (unauthorized users can attack)
- Vulnerability with "User Interaction" value of *None* (no user interaction required)
- Vulnerability with "Availability Impact" value of *High* (can fully shut down the resource)
- A vulnerability has a publicly known exploit via the object property *isExploitedBy*

The full SPARQL query syntax is provided below. This query selects distinct organizations, rather than showing all IP addresses associated with each organization. Each organization could have multiple IP addresses that use the targeted ICS protocols.

```
SELECT
DISTINCT ?Target ?TargetType ?TargetValue ?Protocol ?CVE ?AttackVector ?AttackComplexity ?PrivilegesRequi
red ?UserInteraction ?AvailabilityImpact ?Exploit
WHERE {
        ?Target ics:OrganizationTargetValue ?TargetValue .
                FILTER (?TargetValue = "High") .
        ?Target ics:OrganizationType ?TargetType .
                FILTER (?TargetType = "Education")
        ?Target ics:usesIPAddress ?IPAddress .
        ?IPAddress ics:usesPort ?Port .
        ?Port ics:usesProtocol ?Protocol .
        ?Protocol ics:hasVulnerability ?CVE .
        ?CVE ics:AttackComplexity ?AttackComplexity .
?CVE ics:AttackVector ?AttackVector .
?CVE ics:PrivilegesRequired ?PrivilegesRequired .
?CVE ics:UserInteraction  ?UserInteraction .
?CVE ics:AvailabilityImpact ?AvailabilityImpact .
        FILTER(?AttackVector = "Network" && ?AttackComplexity = "Low" && ?PrivilegesRequired =
        "None" && ?UserInteraction = "None" && ?AvailabilityImpact = "High") .
?CVE ics:isExploitedBy ?Exploit .
}
```

This query, which was completed in 0.3 seconds, produced 155 unique education organizations with the parameters listed above. Table 5 shows example results from this query.

Table 5: Sample query results for high-value education targets that use ICS assets with highly exploitable vulnerabilities and known exploits

Target	Target Type	Target Value	Protocol	CVE	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Exploit	Availability Impact
Wesleyan University	Education	High	BACnet	CVE-2019-12480	Network	Low	None	None	EDB-ID-47148	High
Drexel University	Education	High	BACnet	CVE-2019-12480	Network	Low	None	None	EDB-ID-47148	High
Nova Scotia Dept. of Education	Education	High	BACnet	CVE-2019-12480	Network	Low	None	None	EDB-ID-47148	High
Helena Public Schools	Education	High	BACnet	CVE-2019-12480	Network	Low	None	None	EDB-ID-47148	High
Chery Creek School District	Education	High	BACnet	CVE-2019-12480	Network	Low	None	None	EDB-ID-47148	High

The 155 results included various types of education organizations across the world such as:

- K-12 school districts
- Public and private K-12 schools
- Universities and colleges
- Higher education networks
- University consortiums
- Education departments

The 155 distinct education organizations from the complex SPARQL query represent education organizations that have highly exploitable ICS assets that could be attacked in such a way that the ICS assets can no longer function. Attackers can shut down systems such as physical security systems, heating systems, ventilation systems, fire suppression systems, and other types of ICS systems in K-12 schools, universities, and colleges. Attacks on these ICS systems can significantly disrupt education organizations which can cause a “debilitating effect” overall (CISA, 2020).

In our research project, we started off with 126,636 ICS targets (a Shodan dataset of IP addresses that use ICS protocols) and then used NLP to reduce that list to 2,272 education organizations. However, a list of 2,272 potential targets can still result in several hours of work for ethical hackers in finding highly exploitable education targets. With a complex SPARQL query, we reduced the original target list even further to 155 distinct education organizations that have highly exploitable vulnerabilities with known exploits that can lead to the denial-of-service to critical ICS devices. This reduced the initial Shodan dataset of 126,626 targets by 124,354 targets (98.2%).

Overall, our research showed how semantic-web technologies (ontologies, NLP, and semantic queries) can be used to complete a situation assessment task in ethical hacking (evaluating a list of targets to find education organizations that have highly exploitable vulnerabilities with known exploits). We showed how semantic-web technologies can reduce the information overload faced by cybersecurity professionals (D'Amico et al., 2005; Tyworth et al., 2012; Yen et al., 2010). We also showed how semantic-web technologies can synthesize information together to solve the puzzle of finding targets with specific attributes, all of which represent a situation assessment task (Ben-Bassat and Freedy, 1982). Our results build on previous research that shows how cybersecurity professionals can fuse data from multiple sources to make informed decisions in cyber security (Barford et al., 2010; D'Amico et al., 2005).

5. Conclusion and future work

Evaluating high-value targets based on organization-type, asset-type, and vulnerability data represents a complex situation assessment task for ethical hackers. Initially, we found over 126,000 potential targets that use well-known ICS protocols. With ontology modeling, NLP, and SPARQL queries, we focused on developing reasoning to find education-targets (an example of critical infrastructure targets) that use ICS protocols which are highly susceptible to severe cyber-attacks and that have publicly known exploits. We narrowed down the target list to 155 distinct education targets based on that reasoning. Although our research specifically focused on education targets, the techniques that we utilized in our research can be applied to other critical infrastructure domains.

In future research, we will examine how NLP can be used to identify other types of critical infrastructure targets (such as government organizations) and to evaluate the target value of other types of assets besides ICS assets. To evaluate target values of assets, we will examine how to incorporate various cyber risk frameworks such as the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). Evaluating various types of assets will be critical as ethical hackers could find thousands of assets when scanning a single organization. Overall, our research shows how ontologies can be used to automate situation assessment tasks of ethical hackers as they search for high-value targets including critical infrastructure organizations that use highly exploitable ICS assets.

Acknowledgements

This research is supported, in part, by National Science Foundation Grant No. 1922202, CyberCorps Scholarship for Service (SFS).

References

Angles, R. and Gutierrez, C., 2008, October. "The Expressive Power of SPARQL". International Semantic-web Conference.

Aviad, A., Wecel, K. and Abramowicz, W., 2015, July. "The Semantic Approach to Cyber Security towards Ontology Based Body of Knowledge." European Conference on Cyber Warfare and Security.

Balduccini, M., Kushner, S. and Speck, J., 2015, June. "Ontology-driven Data Semantics Discovery for Cyber-security." International Symposium on Practical Aspects of Declarative Languages.

Barford, P., Dacier, M., Dietterich, T.G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P. and Ou, X., 2010. "Cyber SA: Situational Awareness for Cyber Defense." In Cyber Situational Awareness (pp. 3-13). Springer, Boston, MA.

Ben-Bassat, M. and Freedy, A., 1982. "Knowledge Requirements and Management in Expert Decision Support Systems for (Military) Situation Assessment." IEEE Transactions on Systems, Man, and Cybernetics, 12(4), pp.479-490. CISA, 2020. "Critical Infrastructure Sectors." [online] www.cisa.gov/critical-infrastructure-sectors.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B. and Roth, E., 2005. "Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 49, No. 3, pp. 229-233).

Elliott, T., 2005. "Expert Decision-making in Naturalistic Environments: A Summary of Research."

Endsley, M.R. and Garland, D.J. eds., 2000. Situation Awareness Analysis and Measurement. CRC Press.

Falk, C., 2016. "An Ontology for Threat Intelligence." European Conference on Cyber Warfare and Security.

FBI, CISA, and MS-ISAC, 2020. "Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data." [online] us-cert.cisa.gov/ncas/alerts/aa20-345a

Flowers, A.S., Smith, S.C. and Oltramari, A., 2016. "Security Taxonomies of Industrial Control Systems." In Cyber-security of SCADA and Other Industrial Control Systems (pp. 111-132). Springer, Cham.

Freund, J. and Jones, J., 2014. Measuring and Managing Information Risk: A FAIR approach. Butterworth-Heinemann.

Goodall, J.R., Lutters, W.G. and Komlodi, A., 2009. "Supporting Intrusion Detection Work Practice." Journal of Information System Security, 5(2), pp.42-73.

Gorodetsky, V., Karsaev, O. and Samoilov, V., 2005. "On-line Update of Situation Assessment: A Generic Approach." International Journal of Knowledge-Based and Intelligent Engineering Systems, 9(4), pp.351-365.

Grant, T., van't Wout, C. and van Niekerk, B., 2020. "An Ontology for Cyber ISTAR in Offensive Cyber Operations" European Conference on Cyber Warfare and Security.

Gruber, T.R., 1993. "A Translation Approach to Portable Ontology Specifications." Knowledge Acquisition, 5(2), pp.199-220.

Kirillov, V.P., 1994. "Constructive Stochastic Temporal Reasoning in Situation Assessment". IEEE transactions on Systems, Man, and Cybernetics, 24(8), pp.1099-1113.

Lipshitz, R. and Ben Shaul, O., 1997. "Schemata and Mental Models in Recognition-primed Decision Making." Naturalistic Decision Making, pp.293-303.

Morris, T.H. and Gao, W., 2013, September. "Industrial Control System Cyber-attacks." 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1 (pp. 22-29).

Noble, D., 1993. "A Model to Support Development of Situation Assessment Aids." Decision Making in Action: Models and Methods, pp.287-305.

Noble, D.F., Boehm-Davis, D. and Grosz, C., 1986. "Schema-based Model of Information Processing for Situation Assessment." Engineering Research Associates, Inc., Vienna, VA.

Pérez, J., Arenas, M. and Gutierrez, C., 2006, November. "Semantics and Complexity of SPARQL." International Semantic-web Conference (pp. 30-43).

Rogers, G. and Ashford, T., 2015. "Mitigating Higher Ed Cyber-attacks." Association Supporting Computer Users in Education.

Salas, E., Rosen, M.A. and DiazGranados, D., 2010. "Expertise-based Intuition and Decision Making in Organizations." Journal of Management, 36(4), pp.941-973.

Serfaty, D., MacMillan, J., Entin, E.E. and Entin, E.B., 1997. "The Decision-making Expertise of Battle Commanders." Naturalistic Decision Making, pp.233-246.

Takahashi, T. and Kadobayashi, Y., 2015. "Reference Ontology for Cybersecurity Operational Information." The Computer Journal, 58(10), pp.2297-2312.

Tyworth, M., Giacobe, N. A., Mancuso, V., and Dancy, C. (2012). "The Distributed Nature of Cyber Situation Awareness." In IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA).

Yen, J., McNeese, M., Mullen, T., Hall, D., Fan, X., and Liu, P. (2010). "RPD-based Hypothesis Reasoning for Cyber Situation Awareness." In S. Jajodia (Ed.), Cyber Situational Awareness (pp. 39–49). Springer.

World Wide Web Consortium, 2013. "SPARQL 1.1 Overview." [online] https://www.w3.org/TR/sparql11-overview/

World Wide Web Consortium, 2015. "Semantic Web." [online] from https://www.w3.org/standards/semanticweb/

DR KEITH SCOTT Is Programme Leader for English Language at De Montfort University in Leicester. His research operates at the intersection of communication, culture and cyber, with particular interests in influence, information warfare, and simulations and serious gaming as a training. teaching, and research tool.

Jussi Simola is a doctoral candidate of cyber security at University of Jyväskylä. He received his master degree in Information Systems from the Laurea University of Applied Sciences in 2015. He has worked as a cybersecurity specialist and he has participated in the development of a common Early Warning System for the EU member countries.

Dr. Joshua Alton Sipper is a Professor of Cyberwarfare Studies at the Air Force Cyber College. He completed his Doctoral work at Trident University in September of 2012, earning a Ph.D. in Educational Leadership (emphasis, E-Learning Leadership). Dr. Sipper's research interests include cyber ISR, policy, strategy, and warfare.

Abderrahmane Sokri has a Ph.D. in administration from HEC-Montreal. He is currently serving as economist for the Canadian Department of National Defence. His current research interest includes game theory applied to military operations. He has published in good international journals such as the European Journal of Operational Research.

Sanjana Suresh is a freshman at the LeBow College of Business within Drexel University, majoring in Finance and Business Analytics. She is actively involved in a variety of activities at Drexel, including Drexel's Undergraduate Student Government Association, Drexel Women in Business, and Undergraduate Research. In her free time, Sanjana enjoys spending time with her friends and family, reading, writing, and playing lacrosse.

Professor Iain Sutherland BSc MSc PhD MBCS is currently Professor of Digital Forensics at Noroff University College in Kristiansand, Norway. He is a recognised expert in the area of computer forensics. He has authored articles ranging from forensics practice and procedure to network security. His current research interests lie in the areas of computer forensics and computer security.

Christina Thorpe, B.Sc, Ph.D. Christina Thorpe graduated with a B.Sc. (Hons) in Computer Science from University College Dublin in 2005 and a Ph.D. in Computer Science in 2011. She was a postdoctoral research fellow in the Performance Engineering Lab in UCD from 2011 - 2018. She is currently a Lecturer in Cyber Security in the Technological University Dublin.

Mr. Ilkka Tikanmäki is a researcher at Laurea University of Applied Sciences and a doctoral student of Operational art and tactics at the Finnish National Defence University. He holds an MBA degree in Information Systems and BSc degree in Information Technology.

Maija Turunen is a postgraduate student in military sciences at the Finnish National Defense University. Her main research areas consist of cyber warfare and Russia. Maija Turunen works as a legal counsel at the Finnish Transport Infrastructure Agency.

Brett van Niekerk is a senior lecturer at the University of KwaZulu-Natal. He serves as chair for the IFIP Working Group on ICT in Peace and War, and co-Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He holds a PhD focusing on information operations and critical infrastructure protection.

Namosha Veerasamy: BSc: IT Computer Science Degree, BSc: Computer Science (Honours Degree), MSc: Computer Science with distinction (University of Pretoria) and a PhD (University of Johannesburg). Currently senior researcher (Council for Scientific and Industrial Research in, Pretoria). Qualified as a Certified Information System Security Professional and Certified Information Security Manager. Has been involved in cyber security research and governance for over 15 years.

Gábor Visky is a researcher at NATO CCDCOE, his main field of expertise is industrial control systems. Gábor's previous assignments include 15 years of designing hardware and software for embedded control systems and researching their vulnerabilities through reverse engineering. Gábor holds an MSc degree in Information Engineering with a specialty in Industrial Measurement.