



Delft University of Technology

Developing a Cyber Operations Computational Ontology

Maathuis, C; Pieters, W; van den Berg, J

Publication date

2018

Document Version

Final published version

Published in

Journal of Information Warfare

Citation (APA)

Maathuis, C., Pieters, W., & van den Berg, J. (2018). Developing a Cyber Operations Computational Ontology. *Journal of Information Warfare*, 17(3), 33-52. <https://www.jinfowar.com/journal/volume-17-issue-3/developing-cyber-operations-computational-ontology>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

Green Open Access added to TU Delft Institutional Repository

'You share, we take care!' - Taverne project

<https://www.openaccess.nl/en/you-share-we-take-care>

Otherwise as indicated in the copyright section: the publisher is the copyright holder of this work and the author uses the Dutch legislation to make this work public.

Developing a Cyber Operations Computational Ontology

C Maathuis¹, W Pieters², J van den Berg^{3,4}

¹*Delft University of Technology, TNO,
Netherlands Defense Academy
Delft, Netherlands*

E-mail: clara.maathuis@tudelft.nl

^{2,3}*Delft University of Technology
Delft, Netherlands*

⁴*Leiden University, Netherlands*

E-mail: w.pieters@tudelft.nl; j.vandenberg@tudelft.nl

Abstract: *Cyber operations lack models, methodologies, and mechanisms to describe relevant data and knowledge. This problem is directly reflected when cyber operations are conducted and their effects assessed, and it can produce dissonance and disturbance in corresponding decision-making processes and communication between different military actors. To tackle these issues, this article proposes a knowledge model for cyber operations implemented as a computational ontology following a design science approach grounded on extensive technical-military research. This model classifies the essential entities of cyber operations and was exemplified on three case studies; validation results show that this model can be used to describe cyber operations clearly and concisely.*

Keywords: *Cyber Operations, Cyber Warfare, Cyber Weapons, Cyber Security, Ontology, Artificial Intelligence.*

Introduction

Frederick the Great considered that for war “a great deal of knowledge, study and meditation is necessary to conduct it well” (Luvaas 2001). However, interpreting this quote nowadays can be challenging since societies deal with data, information, and knowledge that empower and revoke participant actors in (un)foreseeable ways. Considering the innovations and advancements in the ICT domain, military actors are able to fight their adversaries in traditional warfare domains, as well as in cyberspace. This is reflected in how they understand, conduct, and deal with cyber operations.

A decade ago—shortly before, during, and shortly after the Russo-Georgian war (August 2008)—a series of cyber operations were conducted against Georgia by undermining its governmental communication capabilities at national and international levels. It was a war planned and conducted on multiple battlefields which impacted Georgia’s national security (Beidleman 2009) and caused significant psychological effects (Shakarian, Shakarian & Ruef

2013). Cyber operations acted as a force multiplier in active combat (Willems 2011) and since then opened long academic debates focused on analysing the incident itself or different aspects through technical, military, or military-legal lenses (Schmitt 2012; Schmitt 2013; Ottis 2015; Barrett 2015).

A decade after, although other cyber operations were conducted, such as the ones in Ukraine, there is still no international consensus regarding their meaning, their definition, or a way to represent them. Currently, different countries are integrating cyber operations into traditional warfare surfaces (Lewis 2015), and these countries acquire or invest in cyber warriors to get the necessary knowledge, skills, and abilities (Li & Daugherty 2015; Arimatsu 2012). Since different actors may be involved in different cyber operations phases, lacking an agreed-upon meaning can directly impact their ability to achieve military objectives.

Addressing both a scientific and societal gap regarding understanding cyber operations, this article began as a piece presented at the 2018 ECCWS conference (Maathuis, Pieters & van den Berg 2018) by providing a supplementary way of using the model as well as a third case study (conducted in Ukraine) for exemplification.

Hence, this article proposes a knowledge model for cyber operations that elaborates and supports the proposed cyber operations definition; provides and shares a common understanding of entities and relations involved in cyber operations by illustrating them in different case studies and in practical use; and raises the level of awareness and responsibility of decision makers, security experts, and academics when reasoning about the effects of cyber operations and contributing to (the process of) designing doctrines, strategies, and methodologies for cyber operations.

The remainder of this article is structured as follows. The second section discusses related research. The third section presents a multidisciplinary definition for cyber operations and stresses the necessity of introducing a model that offers a knowledge-based representation for cyber operations to enable simulation of them in any life-cycle phase. The fourth section discusses the methodology used to design, develop, and evaluate the proposed model—a cyber-operations computational ontology. The fifth section describes the model's design and correspondent decisions for implementation. The sixth section presents the model's implementation in Protégé and illustrates a way to use it. The seventh section presents the validation mechanism, in terms of both technical and expert validation. The eighth section analyses how the model is exemplified in three case studies to reflect its functionality and applicability in real-world settings. The last section discusses possible extensions, reflections, and future research.

Related Research

This research builds on earlier work designed to define cyber operations and to design and develop a knowledge model as a computational ontology that constructs a knowledge base within which to store and represent the knowledge surrounding cyber operations. In recent years, a growing number of studies on ontologies were proposed in the cybersecurity field which aimed to describe notions such as vulnerability, threat, and attack vector (Obrst, Chase & Markeloff 2012; National Institute of Standards and Technology (NIST) 2014; Syed *et al.* 2016), defence technologies (NIST 2014; Ben-Asher *et al.* 2015), digital forensics (Ćosić & Ćosić 2012), intrusion detection (Undercoffer, Joshi & Pinkston 2003), cyber-physical systems (Smirnov, Levashova & Kashevnik 2018; Sun, Liu & Xie 2016) and human factors (Oltamari *et al.* 2015). These studies can also be used to understand some of the entities participating in

cyber warfare, for instance, the vulnerabilities embedded by targets exploited in cyber operations. However, only a limited number of studies aimed at designing ontologies for cyber warfare or conflict exist. Applegate and Stavrou (2013) already identified participant entities in cyberspace conflicts, such as actors and types of impact, but did not formalise them. On modelling network operations, Oltramari *et al.* (2015) propose a theoretical ontology that contributes to predicting and preventing cyberattacks but needs further reflection and extension in real case scenarios in the cyber realm. Furthermore, the initial stage of a cyber-network attack-planning ontology aiming at supporting the planning of cyber operations was introduced by Chan *et al.* (2015).

As this article interprets and embeds the Computer Science and Artificial Intelligence sense of an ontology, a series of prerequisites must be fulfilled to enable the design, development, and evaluation of the ontology. Since both cyber security and military reasoning are considered by Dipert (2013), his proposed requirements, which are both universal and widely applicable, were adopted in this research. Dipert scrutinised these requirements in order to support the development of a fundamental ontology for cyber warfare for standardisation purposes.

Methodology

To be able to formalise cyber operations by means of a computational ontology, this research relies on different multidisciplinary resources in a triangulating manner (Yin 2003). Ontology Engineering translates the philosophical understanding of ontology to the Computer Science and Artificial Intelligence domains by using different methodologies to implement a computational ontology. The ‘methontology’ methodology (Fernández-López, Gómez-Pérez & Juristo 1997) was selected for use because it is grounded in an extensive survey of literature, reports, and military doctrine, combined with direct participation and observation in joint military exercises. At the same time, the necessary features of a cyber warfare ontology proposed by Dipert (2013) were followed. Additionally, one of the authors’ experience in planning and conducting cyber operations as (cyber) war games resonates in the mechanism of conducting in-depth case studies on Georgia, Iran (Stuxnet), and Ukraine as exemplifying cases for the proposed model.

Ontology engineering methodologies are used to design formal models of different domains and aspects of reality by constructing a knowledge base, conceptualising the world of interest, and proposing definitions of entities and relationships, which not only allows knowledge to be accumulated, computed, and accessed, but also shared among different audiences and communities (Fernández-López, Gómez-Pérez & Juristo 1997; Mizoguchi & Ikeda 1998; Roussey *et al.* 2011; d’Aquin, Kronberger & Suarez-Figueroa. 2012).

The methodology in this research was selected because it is also one of the most comprehensive and used Ontology Engineering methodologies (Paquette 2010). This methodology presupposes implementing computational ontologies from scratch or using existing ones, is fully compatible with *IEEE 1074-2006 Standard for Developing Software Project Life Cycle Process*, and is aligned with the requirements of Dipert (2013). Furthermore, each phase of the followed methodology is elaborated as follows (Fernández-López, Gómez-Pérez & Juristo 1997; Sawsaa & Lu 2012):

- Specification The purpose, requirements, and knowledge are established to represent cyber operations as military operations.
- Knowledge acquisition The necessary information for building the model is collected from the abovementioned resources.

- Conceptualisation The knowledge gathered is structured as a formal model in the form of a taxonomy with concepts, meanings, and attributes that describe cyber operations.
- Formalisation The knowledge model is formalised and has the following classes: Context, Actor, Type, MilitaryObjective, Phase, Target, CyberWeapon, Asset, Geolocation, Action and Effect.
- Integration Other ontologies were reviewed and are presented in the Related Work section. However, the proposed ontology was designed from scratch.
- Implementation The knowledge engineering environment for building intelligent systems—Protégé—is prepared to develop the model using Ontology Web Language (OWL) and describe the knowledge about entities, groups of entities, and relations between entities.
- Maintenance The model is refined and updated so that actions such as modifying, adding, and removing concepts and definitions are possible.
- Evaluation The structure/consistency evaluation and the military experts' evaluation are carried out together with exemplification on three real cases of cyber operations performed in Georgia, Iran (Stuxnet), and Ukraine.
- Documentation- This phase occurs during the entire process of design and development of the new model and requires a detailed description of contained concepts and relations between these concepts. Such a description is presented in the following section.

Defining Cyber Operations

Most conflicts do not involve just state-on-state military confrontations (Brown 2017). Non-state actors can also conduct cyber operations, which can lead to global (and even devastating) implications and consequences impacting not only the targeted adversaries, but also other actors such as the neutral or friendly ones, and even the attackers themselves. Caton (2015) argues that cyber operations “have been ongoing since before the advent of the Internet, and their influence on traditional Military Operations continues to increase”. Indeed, they can be found now globally integrated into military commanders' toolboxes as means and methods to achieve political goals and military objectives by synchronising activities and actions in all warfare domains.

This research is aligned with the vision of Herr and Herrick (2016), which stresses the need for understanding cyber operations and describes them as “the acquisition and use of cyber capabilities at the strategic, operational, and tactical levels of conflict”. To that end, the present article calls for a unified definition for cyber operations before engaging in designing and developing a model that represents its surrounding knowledge and serves as a knowledge-based simulation environment useful in all its life cycle phases. At the same time, this definition is necessary because the level of awareness and reasoning of the participating communities (cyber, military, military-legal) needs to be raised to insure the unification of effort between the different experts who compose them. Therefore, the following multidisciplinary definition of ‘cyber operation’ is essential and is proposed based on extensive review of scientific literature, reports, and military doctrine:

A cyber operation is a type of or a part of a military operation in which cyber weapons/capabilities are used to achieve military objectives in front of adversaries inside and/or outside cyberspace.

The following applies to the proposed definition:

- As ‘a type of or a part of a military operation’, a cyber operation can be either an independent military operation or a part of a broader military operation in a supporting role.
- ‘Cyber weapons/capabilities’ are programs or scripts employed to achieve military objectives (Maathuis, Pieters & van den Berg 2016).
- ‘To achieve military objectives’ implies to accomplish military goals by engaging targets in cyber operations.
- ‘In front of adversaries’ refers to the opponents participating in the conflict.
- ‘Inside and/or outside cyberspace’ recognises that although cyber operations act on different cyberspace entities, their effects are borderless since they cross geographical and virtual borders. They impact targets as well as collateral assets which are distinct from the engaged targets.

Model Design

The Methodology section presented the approach followed in this research. Hence, to be able to understand the rationale behind the design of the proposed model, the design requirements and the followed design decisions are described here. This research follows the requirements for a cyber warfare ontology established by Dipert (2013) along with experience writing cyber operations scenarios, and direct participation and observation in joint military operations exercises, facts also reflected in other lines of research. To the best of the authors’ knowledge, this set of requirements is the only one proposed in the existing scientific literature, and these authors introduced a computational ontology for cyber operations for the first time in 2018.

The design requirements considered by Dipert (2013) are

- to be humanly understandable by using controlled vocabularies;
- to be an ontology that uses widely known and accepted concepts;
- to be represented in one of the best available languages for formalising ontologies, such as OWL or Common Logic; and
- to be able to apply methodologies for building ontologies and for illustrating instance-level data.

At the end of these phases, the taxonomical representation of the proposed model contains the following upper classes: Context, Actor, Type, MilitaryObjective, Phase, Target, CyberWeapon, Asset, Geolocation, Action and Effect. These classes map the components of the proposed definition for cyber operations and are depicted in **Table 1**, below.

Elements of the cyber operations definition	Mapping on cyber operations upper classes
A type of a part of a military operation	Context, MilitaryObjective
Cyber weapons/capabilities	CyberWeapon
To achieve military objectives	Context, MilitaryObjective, Type, Phase
In front of adversaries	Actor, Type, Phase, Target, Geolocation
Inside and/or outside cyberspace	Target, Geolocation, Asset, Effect

Table 1: Mapping between the components of the proposed cyber operations definition and the upper classes of the proposed model

The first four phases of the methodological approach—specification, knowledge acquisition, conceptualisation and formalisation—are the steps followed to design the artefact (computational ontology model) in a design science approach (Hevner, March & Park 2004).

Furthermore, each upper class was elaborated to consider concepts and relations (subclasses and properties) between them in the way of representing its knowledge using known and accepted concepts from cyber, military, and military-legal domains. Consequently, the initial design of the proposed ontology was established and proposed for evaluation.

Model Implementation and Use

Once the initial design was established, the ontology was further developed in the knowledge engineering environment named Protégé as a set of structured concepts together with relationships between these concepts organised in a logical way. Afterwards, the double process of evaluation (technical and expert based) was carried out, and small changes were applied to Actor and Target classes. These changes are presented in the Validation section. Therefore, the final form of the proposed model was accordingly implemented; contains 140 classes, 53 individuals (instances), and 96 (55 data and 41 object) properties; and is depicted in **Figure 1**, where classes marked with + are further extended (contain other sub-classes), with its metrics presented in **Figure 2**.

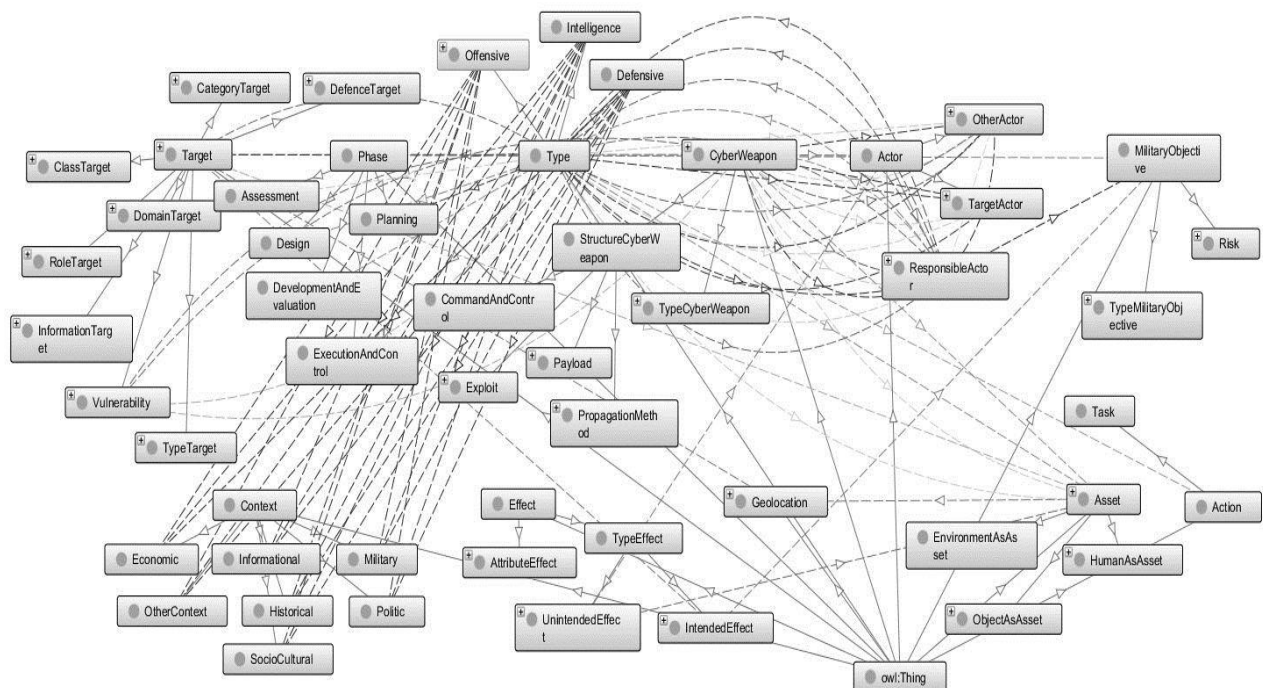


Figure 1: Cyber operations ontology classes hierarchy

Ontology metrics:	
Metrics	
Axiom	965
Logical axiom count	554
Declaration axioms count	287
Class count	140
Object property count	41
Data property count	55
Individual count	53

Figure 2: Cyber operations ontology metrics

Ontologies represent a context-dependent projection of a reality. In this way, the proposed ontology is organised as a collection of entities that describe the universe of cyber operations structured on four levels, as discussed below.

Level 1 contains the upper classes as shown in **Figure 3**, below. They are mapped based upon the concept of cyber operations, specifically the use of cyber weapons as described by United States Army (2013), Williams (2014), and by Maathuis, Pieters & van den Berg (2016).

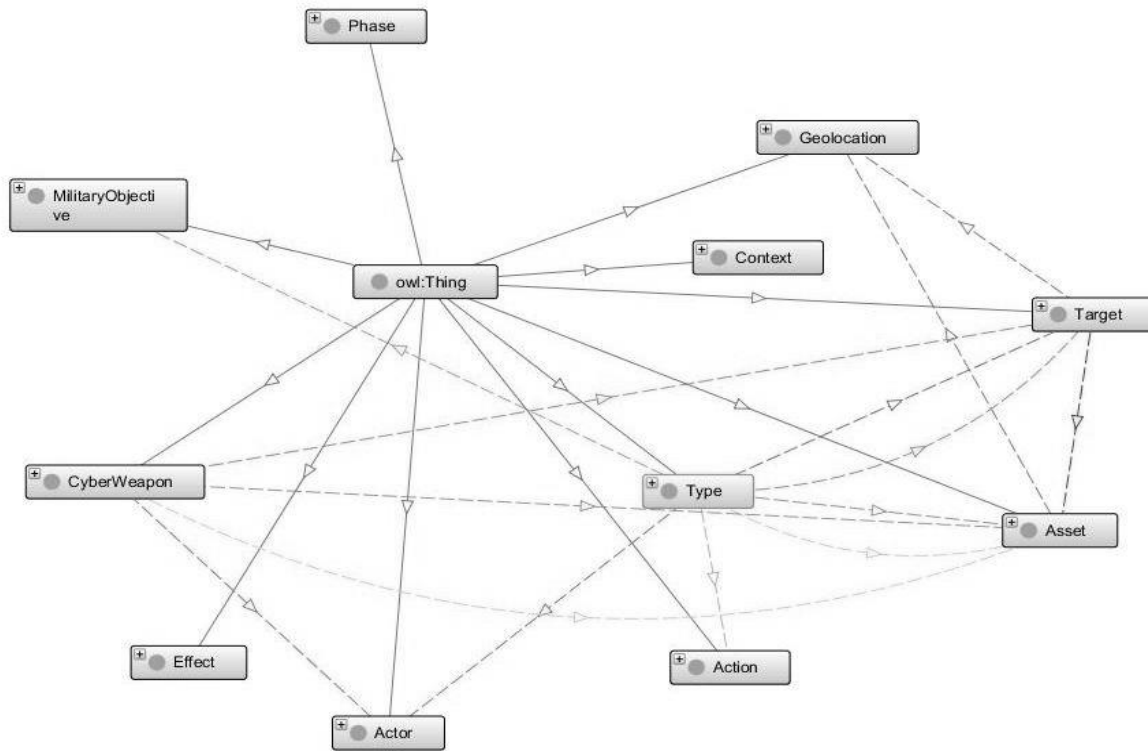


Figure 3: Cyber operations ontology upper classes

The classes are described as follows:

1. Context: the following dimensions: Political, Military, Economic, Informational, Historical, Sociocultural, and Other Context (in keeping with Arimatsu's 2012 argument that a broader context needs to be considered for cyber operations).
2. Actor: distinct types of actors who are either responsible for planning, executing, or assessing cyber operations are the targeted ones or the ones unintentionally impacted by cyber operations.
3. Type: distinct types of cyber operations, specifically offensive, defensive, and intelligence (United States Army 2013; Williams 2014).
4. MilitaryObjective: the military goal that actors want to achieve in cyber operations (Theonary & Harrington 2015).
5. Phase: the phases of cyber operations from planning to assessment.

6. Target: a military entity (person or object) legally targetable in cyber operations (Liles *et al.* 2012).
7. CyberWeapon: the means employed in cyber operations to achieve military objectives.
8. Asset: either humans or objects unintentionally impacted in cyber operations.
9. Geolocation: incorporated geolocation information about targets or assets.
10. Action: the actions and tasks involved or performed in cyber operations.
11. Effect: the implications and consequences of cyber operations. The intention criterion is decisive when classifying the effects of cyber operations: intended effects that support the achievement of military objectives (Military Advantage) by targets' engagement; and unintended effects that do not contribute to the achievement of military objectives, but do still unintentionally impact other assets (for instance, Collateral Damage).

Level 2 contains the sub-classes that extend and describe the upper classes, such as Offensive, Vulnerability, Exploit, and UnintendedEffect. **Level 3** contains the individual (instances) of classes that compose the ontology. This ontology, applied to cyber operations conducted in Georgia, Iran (Stuxnet) and Ukraine, is depicted in **Figure 4**, below.



Figure 4: Cyber operations ontology individuals

Level 4 contains the relationships between classes and individuals, as well as links between individually named data and object properties, as depicted in **Figure 5**, below.

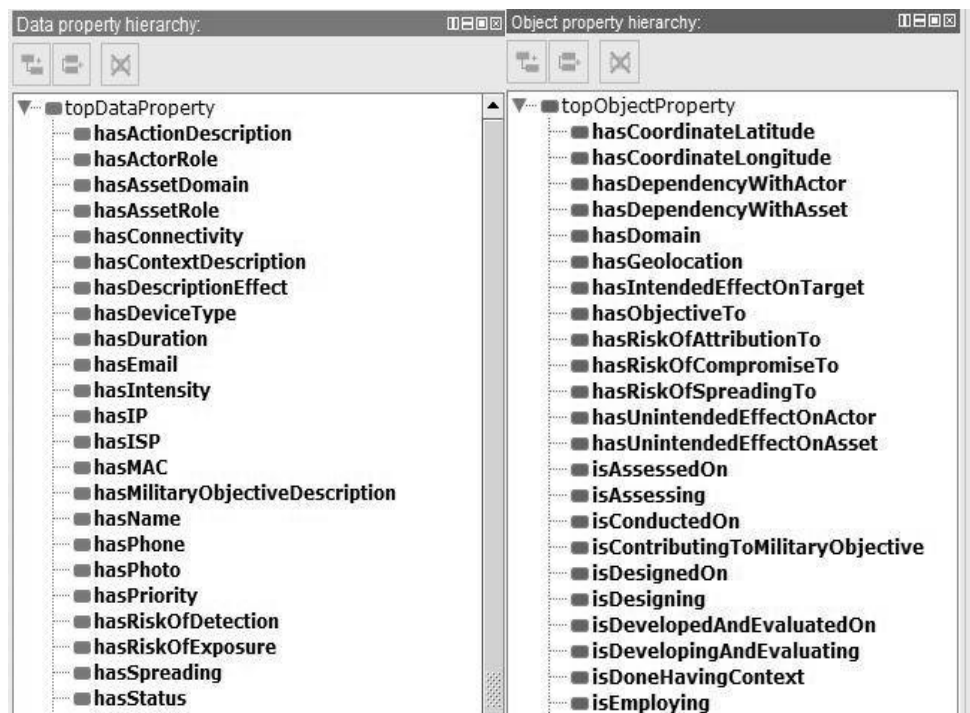


Figure 5: Cyber operations ontology data and object properties

The four data and object properties are described as follows:

- ‘hasMilitaryObjectiveDescription’ represents the military objective that needs to be achieved.
- ‘isExploiting’ reflects which vulnerability is exploited.
- ‘isDeliveringMilitaryAdvantage’ verifies whether or not a target delivers a military advantage.
- ‘isProducingCollateralDamage’ checks if collateral damage is produced by engaging a target.

Therefore, the entire universe of cyber operations can be depicted as a complete picture, as shown in **Figure 6**, below.

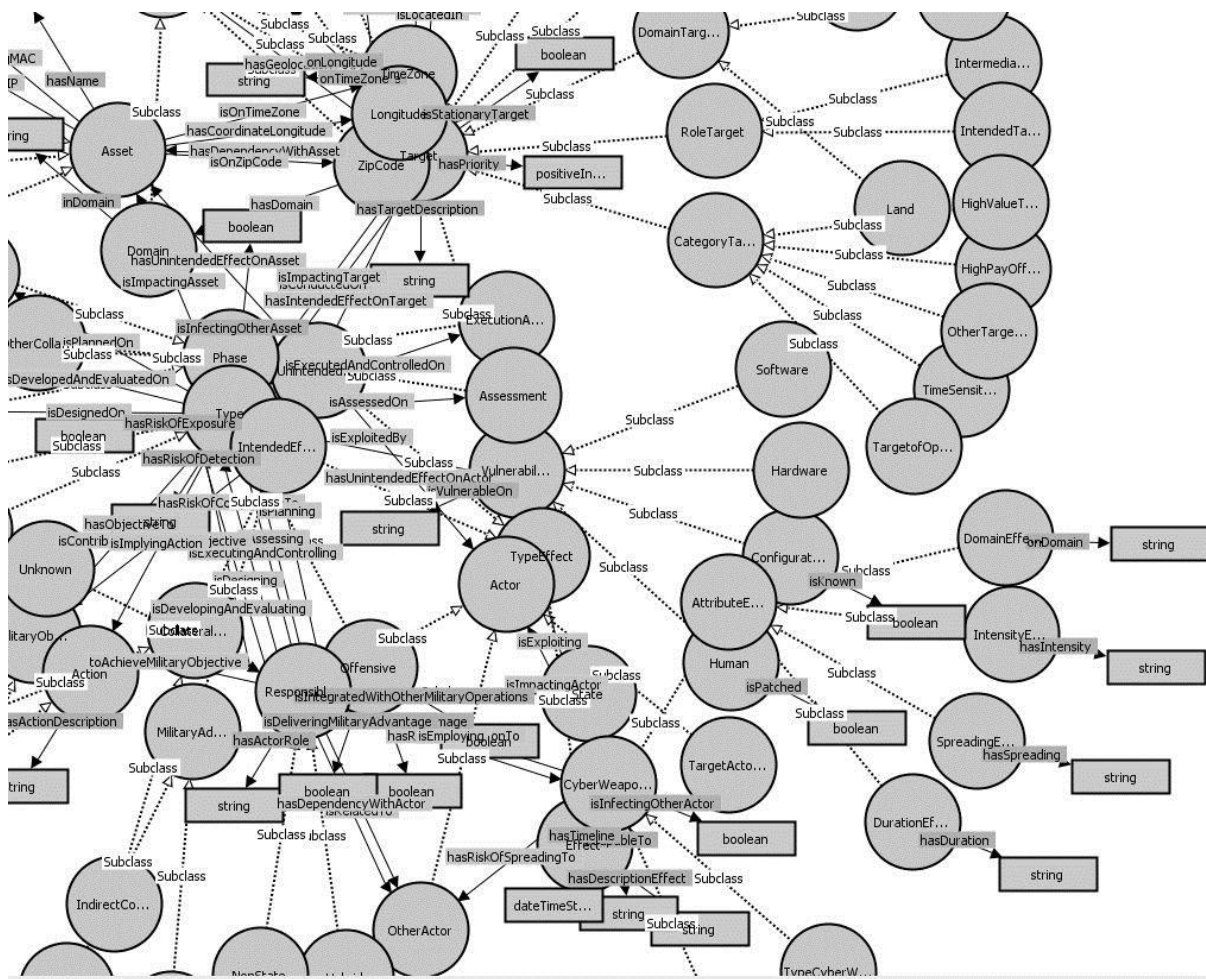


Figure 6: Cyber Operations universe containing classes and sub-classes, plus data and object properties

Ontologies are used effectively to model knowledge and deal with its representation and retrieval (Munir & Anjum 2017). It is important to mention that OWL has the highest level of expressivity compared to similar standards or languages, and allows great machine interpretability. It is also the AI-based ontology implementation language considered as a requirement by Dipert (2013). However, no matter which syntax is used to design and develop an ontology (OWL, JSON [Java Script Object Notation], Turtle, for example), there are several ways of using it to allow automated extraction and visualisation. Furthermore, a way is presented using the SPARQL (Sparql Protocol and RDF Query Language) in Protégé. To illustrate, a query for extracting all classes, their subclasses, and individuals is depicted below in **Figure 7**, below.

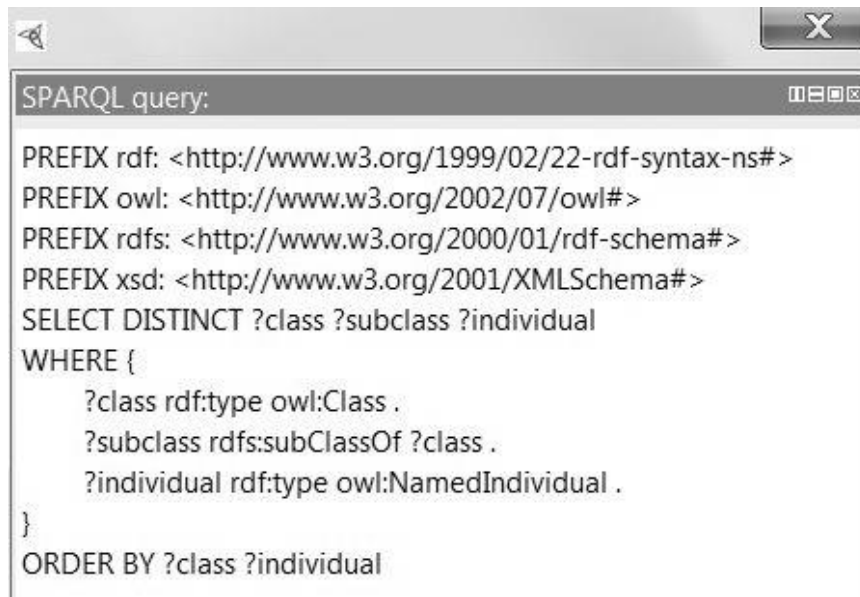


Figure 7: Example of SPARQL query for cyber operations ontology

This query can also be adapted to extract the exploitable vulnerabilities for considered targets using clauses such as `OPTIONAL` and `FILTER`.

Model Validation

There are two ways of evaluating and validating a developed ontology: technically based or expert based (Sawsaa & Lu 2012). To make sure that the proposed model represents cyber operations in an accurate, clear, and concise way, both evaluation mechanisms were applied. This model is also exemplified by instantiation based on three case studies of cyber operations conducted in Georgia, Iran (Stuxnet), and Ukraine.

The technical evaluation applied considered indicators such as consistency and reusability (Sawsaa & Lu 2012; Esposito, Zappatore & Tarricone 2011) and was successful using the Hermit reasoner. The expert evaluation was conducted in a few rounds of meetings and reviews with two military experts who had extensive international experience in missions and operations. For the expert evaluation, indicators such as accuracy, clarity, conciseness, and adaptability (Vrandečić 2009; Sawsaa & Lu 2012) were considered. Applying these criteria and stressing again the necessity of representing the knowledge that would assist and simulate cyber operations, the experts welcomed and agreed with the proposed model. After consideration, the experts recommended making minor changes, and the model was updated accordingly in the following three ways:

1. Introducing ‘target’s role’ in the sense of intended targets that can be attacked directly or through intermediary targets (Target class).
2. Introducing ‘targets of opportunity’ as well as other possible targets (Target class).
3. Introducing ‘Unknown actor’ in recognition of the fact that limited to no information might be available to help attribute a cyber operation to an actor (Actor class).

After these updates were incorporated, the model reached its final state and met all the requirements of a cyber-warfare ontology as proposed by Dipert (2013).

Case Studies of Cyber Operations

To exemplify the proposed model, three use cases were created based on extensive case study research (Yin 2003) on cyber operations conducted in Georgia, Iran (Stuxnet), and Ukraine. Furthermore, each case study was briefly described. The case study regarding Georgia focused on the cyber operations conducted in 2008 surrounding the war between Russia and Georgia, that aimed at isolating or limiting Georgian communications of political and public assets at national and international levels. The case study focusing on Iran addressed the series of cyber operations or what can be seen as a long-term cyber operation discovered in 2010 (Operation Olympic Games/Stuxnet) conducted on Iranian nuclear facilities with the purpose of reducing the nuclear enrichment productivity as part of Iran's nuclear program. The case study with regard to Ukraine focused on the cyber operation (Black Energy 3) carried out in 2015 in Ukraine that targeted the Ukrainian power grid through different electricity distributors in Ivano-Frankivsk. Hence, **Table 2**, below, summarises all three case studies in order to exemplify both the proposed model and definition for cyber operations.

The goal of these case studies is to provide guidance and support to military and policy decision-makers when they encounter difficulties in understanding and comprehending cyber operations. As this model explicitly reveals its main characteristics, it also plays an important role in clarifying the cyber-operations phenomenon. Its use on these three case studies proves its effectiveness and applicability to real-world situations. Additionally, it exposes the strong relationships between entities such as Context, MilitaryObjective, and Effect since a MilitaryObjective finds its roots and motivations in the Context of a cyber operation, and the intended effects contribute to achieving the MilitaryObjective. Hence, these aspects are depicted for all three cases in **Table 2**, below, and demonstrate above all that the context of a cyber operation cannot be divorced from the cyber operation itself if one wants to comprehend the effects. In other words, the implications and consequences of cyber operations.

Class	Georgia (Grigolia 2008; Swanson 2010; Tikk et al. 2008; Nazario 2009; Hollis 2011; Mshvidobadze 2015)	Iran (Stuxnet) (Albright 2003; Avramovic 2007; Albright, Brannan & Shire 2008; Langner 2013; Falliere, Murchu & Chien 2011; McDonald et al. 2013; Albright et al. 2012; Zetter 2015)	Ukraine (Black Energy 3) (SANS 2016; Fire Eye 2016; GReAT 2016; Liang et al. 2017; Damsky 2016; Shamir 2016; Sun, Yang & Zhou 2016; Department of Homeland Security 2016)
Context	Political: tensions grounded on the independence aim of two Georgian regions, Abkhazia and South Ossetia supported by Russia. Military: Russo-Georgian war.	Political: tensions regarding the development of Iran's nuclear program. Military: the possibility of Iran investing in its nuclear program for military purposes.	Political: tensions grounded on the Russian annexation of Crimea and further resistance and protests. Military: a possible proof or demonstration of 'show of force', reply to previous Ukrainian activities, all backed by revealing and exploiting civilian/societal vulnerabilities.
Actor	Russia vs Georgia	U.S. and Israel vs Iran	SandWorm (Russia) vs Ukraine
Type	Offensive	Offensive	Offensive
Military Objective	To (digitally) isolate Georgia and disrupt its ICT communications through governmental,	To delay Iran's nuclear program.	To disrupt the information systems of three electricity distributors in order to produce service outages, a

	media and financial websites.		societal discomfort and influence public opinion.
Phase	Assessment	Assessment	Assessment
Target	Georgia's communication systems of governmental, media and financial institutions by exploiting software and configuration vulnerabilities.	Iran's nuclear facilities/program by exploiting software and human vulnerabilities.	Ukrainian power grid and electricity distribution companies in the Ivano-Frankivsk region.
Cyber Weapon	Georgia	Stuxnet	Black Energy
Asset	Other systems and people/society.	Other facilities, systems and people/society.	Other facilities, systems and people/society.
Geolocation	Target: in Georgia. Asset: global (for example Georgia, Russia, Azerbaijan, U.S.)	Target: in Iran. Asset: global (for instance Indonesia, India, U.S.)	Target: in Ukraine. Asset: local and national (in Ukraine).
Action	(Part of) A Military Operation that took place around the war between the involved parties.	(Possible part of) A Military Operation that did not take place during war.	(Possible part of) A Military Operation that took place during the conflict in Eastern Ukraine and extended influential areas.
Effect	Intended: isolation, confusion and inconvenience in Georgia, as well as limiting communications access and use. Unintended: communications denial in supportive countries.	Intended: damage or destroy nuclear enrichment centrifuges by sabotaging them. Unintended: infecting other facilities and systems.	Intended: disruption or damage of power grid information systems. Unintended: future escalation and global exposure.

Table 2: Case studies exemplifying the proposed ontology for cyber operations

Conclusions

As different actors are integrating cyber operations in their military theatre of operations, it is necessary to understand what these new types of operations are to be able to represent and simulate, and it is necessary to understand how to use them properly to further deal with the effects of their actions. A way to do this was presented in this article as a joint venture of theoretical, empirical, and practical efforts. Hence, a knowledge model for cyber operations was proposed as a computational ontology in a design science approach implemented in Protégé. In this way, understanding, flexibility, and reusability (Tolk & Smith 2011; Sawsaa & Lu 2012) for composing entities and parties involved are ensured.

This article overcomes the current limits of the state of the art and contributes to the body of knowledge of cyber and military domains, and to the efforts of decision makers, security experts, and academic researchers when understanding what these operations mean and how to plan them or assess their effects. The results of this research accomplished the cyber warfare ontology requirements considered by Dipert (2013), were successfully evaluated technically and by military experts, and were exemplified on three cyber-operations case studies on Georgia, Iran (Stuxnet), and Ukraine.

This research also contributes to the existing body of knowledge of Artificial Intelligence and Computer Science domains, and calls for their involvement when conducting research in

Knowledge Modelling useful in emerging or complex assessments and decision-making processes. Possible extensions of this work can be considered by elaborating the classes Context and Effect to define more context dimensions and domains, attributes, and metrics of effects. Other extensions are also possible in the sense of representing Hybrid Warfare/Operations using (at least) the same upper classes structure to be able to (better) understand and represent different types of hybrid threats, ends, ways, and means.

An intrinsic limitation is that, when representing knowledge in the form of an ontology, there is not just one form that it can take since the knowledge representation formalism consists of different kinds of representations, depending on the perspective(s) and vision(s) that one has. An extrinsic limitation is that this model was instantiated using just three use cases due to the limited number of incidents publicly known and, implicitly, available empirical data(sets).

The proposed model represents a *machete* that can be further elaborated to understand, represent, and simulate current and new types of operations in all phases of their life cycles. The authors will be using these findings in their future research concerning the design of models and methodologies for assessing the effects of cyber operations.

Acknowledgement

We would like to thank to Drs. Rudi Gouweleeuw MAJ(R) and Prof. Dr. Paul Ducheine BG for their useful feedback and support.

Note

This publication is an updated version of the paper ‘A Computational Ontology for Cyber Operations’, which was presented at the 17th European Conference on Cyber Warfare and Security, ECCWS, University of Oslo, Oslo, Norway, 28-29 July 2018.

References

Albright, D 2003, *Iran at a nuclear crossroads*, Institute for Science and International Security (ISIS), viewed 12 November 2017, <<http://isis-online.org/publications/iran/crossroads.html>>.

Albright, D, Brannan, P & Shire, J 2008, *Can military strikes destroy centrifuge program? Probably not*, ISIS, viewed 12 November 2017, <https://www.isis-online.org/publications/iran/Centrifuge_Manufacturing_7August2008.pdf>.

Albright, D, Brannan, P, Stricker, A, Walrond, C & Wood, S 2012, *Preventing Iran from getting nuclear weapons: Constraining its future nuclear options*, ISIS, viewed 12 November 2017, <https://isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf>.

Avramovic, J 2007, *Iran's nuclear program: What the 2008 presidential candidates are saying*, ISIS, viewed 13 November 2017, <<http://www.isis-online.org/publications/iran/PresidentialCandidates.pdf>>.

Applegate, SD. & Stavrou, A 2013, ‘Towards a cyber conflict taxonomy’, *Proceedings of the 5th Conference on Cyber Conflict (CyCon)*, IEEE, pp. 1-8.

Arimatsu, L 2012, ‘A treaty for governing cyber weapons: Potential benefits and practical limitations’, *Proceedings of the 4th conference on Cyber Conflict (CyCon)*, IEEE, pp. 1-19.

Barrett, ET 2015, Reliable old wineskins: The applicability of the just war tradition to military cyber operations', *Philosophy and Technology*, vol. 28, no. 3, pp. 387-405.

Beidleman, SW 2009, 'Defining and deterring cyber war', Defense Technical Information Center, viewed 10 October 2017, <<http://www.dtic.mil/docs/citations/ADA500795>>.

Ben-Asher, N, Oltramari, A, Erbacher, RF & Gonzales, C 2015, 'Ontology-based Adaptive Systems of Cyber Defense', *STIDS*. pp. 34-41.

Brown, J 2017, *Making sense of irregular war*, Over the horizon: Multi-Domain operations & Strategies, 19 April, viewed 1 December 2017, <<https://overthehorizonmdos.com/2017/04/19/making-sense-of-irregular-war/>>.

Caton, JL 2015, *Army support of military operations: Joint contexts and global escalation implications*, USAWC SSI, viewed 6 November 2017, <<http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1246>>.

Chan, P, Theron, J, van Heerden, R & Leenen, L 2015, 'An ontological knowledge base for cyber network attack planning', *Proceedings of the 10th International Conference on Cyber Warfare and Security, ICCWS*, p. 69.

Ćosić, J, & Ćosić, Z 2012, 'The necessity of developing a digital evidence ontology,' *Proceedings of the Central European Conference on Information and Intelligent Systems*, pp. 325-30.

Damsky, I 2016, *Black Energy Security Report*, ThreatSTOP, February 2016, viewed 3 November 2017, <https://threatstop.com/sites/default/files/ThreatSTOP_BlackEnergy.pdf>.

Department of Homeland Security 2016, *Alert (IR-ALERT-H-16-056-01): Cyber-Attack against Ukrainian critical infrastructure*, U.S. Industrial Control Systems Cyber Emergency Response Team, 25 February 2016, viewed 12 November 2017, <<https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>>.

Dipert, R 2013, 'The essential features of an ontology for cyberwarfare', *Conflict and cooperation in cyberspace*, P Yannakogeorgos & A Lowther (eds), Taylor & Francis, London, UK, pp.35-48.

d'Aquin, M, Kronberger, G & Suarez-Figueroa, MC 2012, 'Combining data mining and ontology engineering to enrich ontologies and linked data', *Proceedings of the first international workshop on Knowledge Discovery and Data Mining Meets Linked Open Data (KNOW@LOD)*, vol. 868, CEUR Workshop Proceedings, pp. 19-24.

Esposito, A, Zappatore, M & Tarricone, L 2011, 'Evaluating scientific domain ontologies for the electromagnetic knowledge domain: A general methodology', *Journal of Web & Semantic Technology*. vol. 2, no. 2, pp. 1-19.

Falliere, N, Murchu, L & Chien, E 2011, *W32.Stuxnet dossier, version 1.4*, Symantec Security Response, February, Cupertino, CA, US.

Fernández-López, M, Gómez-Pérez, A & Juristo, N 1997, 'Methontology: From ontological art towards ontological engineering', *Proceedings of the fourteenth national conference on Artificial Intelligence, AAAI-97*, Spring Symposium Series, pp. 33-40.

Fire Eye 2016, *Cyber attacks on the Ukrainian grid: What you should know*, Fire Eye Industry Intelligence Report, Milpitas, CA, US.

GReAT 2016, *Black Energy APT attacks in Ukraine employ spearphishing with Word documents*, Securelist, 28 January, viewed 17 September 2018, <<https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/>>.

Grigolia, G 2008, *Georgia 2008: Legal evaluation according to Georgian and International law*, Cyber Security Bureau Georgia, viewed 15 November 2017, <<http://csbd.gov.ge/doc/labour/Georgia-2008-Legal-Evaluation-According-To-Georgian-And-International-Law.pdf>>.

Herr, T & Herrick, D 2016, 'Military cyber operations: A primer', *The American Foreign Policy Council*, 30 January, American Foreign Policy Council Defense Technology Program Brief, no. 14, January 2016, viewed 17 September 2018, <<https://ssrn.com/abstract=2725275>>.

Hevner, AR, March, ST & Park, J 2004, 'Design research in information systems research', *MIS Quarterly*, vol. 28, no. 1, pp. 75-105.

Hollis, D 2011, 'Cyberwar case study: Georgia 2008', *Small Wars Journal*, viewed 03 December 2017, <<http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>>.

Langner, R 2013, *To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve*, The Langner Group, Arlington, US, and Hamburg/Munich, DE.

Lewis, J 2015, 'The role of offensive cyber operations in NATO's collective defence', *The Tallinn Papers*, no. 8, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, EE.

Li, J & Daugherty, L 2015, *Training cyber warriors: What can be learned from defense language training?*, RAND, Santa Monica, CA, US.

Liang, G, Weller, SR, Zhao, J, Luo, F & Dong, ZY 2017, 'The 2015 Ukraine blackout: Implications for false data injection attacks', *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-8.

Liles, S, Dietz, JE, Rogers, M & Larson, D 2012, 'Applying traditional military principles to cyber warfare', *Proceedings of the 4th international conference on Cyber Conflict (CyCon)*, IEEE, pp. 1-12.

Luvaas, J. 2001, *Napoleon on the Art of War*, Simon and Schuster, New York, NY, US, pp. 21.

Maathuis, C, Pieters, W & van den Berg, J 2016, 'Cyber weapons: A profiling framework', *Proceedings of the 1st international conference on Cyber Conflict (CyCon US)*, IEEE, pp. 1-8.

———2018, ‘A computational ontology for cyber operations’, *Proceedings of the 17th International Conference on Cyber Warfare and Security, ICCWS*, pp. 278-88.

McDonald, G, Murchu, LO, Doherty, S & Chien, E 2013, *Stuxnet 0.5: The missing link*, Symantec Security Response, Cupertino, CA, US.

Mizoguchi R & Ikeda, M 1998, ‘Towards ontology engineering’, *Journal of the Japanese Society for Artificial Intelligence*, vol. 13, pp. 9-10.

Mshvidobadze, K 2015, *Georgia cyber barometer report*, Rondeli Foundation: Georgian Foundation for Strategic and International Studies, Tbilisi, GE.

Munir, K & Anjum, MS 2017, ‘The use of ontologies for effective knowledge modelling and information retrieval’, *Applied Computing and Informatics*, vol. 14, no. 2, pp. 116-26.

Nazario, J 2009, ‘Political motivated Denial of Service attacks’, *The virtual battlespace: Perspectives on cyber warfare*. eds. C Czosseck & K Geers, IOS Press, Amsterdam, NL, pp.163-181.

National Institute of Standards and Technology (NIST) 2014, *Framework for improving critical infrastructure cybersecurity, version 1.0*, 12 February, NIST Cybersecurity Framework, Gaithersburg, MD, US.

Obrst, L, Chase, P & Markeloff, R 2012, ‘Developing an ontology of the cyber security domain’, *STIDS*, pp. 49-56.

Oltramari, A, Cranor, LF, Walls, RJ & McDaniel, P 2015, ‘Computational ontology of network operations’, *Proceedings of the Military Communications Conference*, IEEE, pp. 318-23.

Ottis, R 2015, ‘Cyber warfare’, *Cyber security: Analytics, technology and automation*, M Lehto & P Neittaanmäki, (eds), Springer, eBook, ISBN 978-3-319-18302-2.

Paquette, G 2010, *Visual knowledge modeling for semanting web technologies: Models and ontologies*, Information Science Reference, IGI Global, Hershey, PA, US.

Roussey, C, Pinet F, Kang, MA & Corcho O 2011, ‘An introduction to ontologies and ontology engineering’, G Falquet, C Métral, J Teller & C Tweed (eds), *Ontologies in urban development projects*, vol. 1, Springer, London, UK, pp. 9-38.

SANS Industrial Control Systems (ICS) 2016, *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*, 18 March, Electricity Information Sharing and Analysis Center (E-ISACSANS), Washington, DC, US.

Sawsaa, AF & Lu, J 2012, ‘Building information science ontology (OIS) with Methontology and Protégé’, *Journal of Internet Technology and Secured Transactions*, no. 1, vol. 3/4.

Schmitt, M 2012, “‘Attack’ as a term of art in international law: The cyber operations context”, *Proceedings of the 4th international conference on Cyber Conflict (CyCon)*, IEEE, pp.1-11.

——(ed.) 2013, *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press, Cambridge, UK.

Shakarian, P, Shakarian, J & Ruef, A 2013, *Introduction to cyber-warfare: A multidisciplinary approach*, Elsevier, Amsterdam, NL.

Shamir, U 2016, *Analyzing a new variant of Black Energy 3: Likely insider-based execution*, Executive Summary, Sentinel One, Mountain View, CA, US.

Smirnov, A, Levashova, T & Kashevnik, A 2018, 'Ontology-Based resource interoperability in socio-cyber-physical systems', *IT in Industry*, vol. 6, no. 2, pp. 19-24

Sun, Y, Yang, G, & Zhou, X 2016, 'A novel ontology-based service model for cyber physical system', *Proceedings of the 5th international conference on Computer Science and Network Technology*, IEEE, pp. 125-131.

Sun, CC, Liu, CC & Xie, J 2016, 'Cyber-Physical system security of a power grid: State-of-the-art', *Electronics*, vol. 5, no. 3, p. 40.

Swanson, L 2010, 'The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict', *Loyola of Los Angeles International and Comparative Law Review*, p. 303-33.

Syed, Z, Padia, A, Finin, T, Mathews, L & Joshi, A 2016, 'UCO: A Unified Cybersecurity Ontology', *Proceedings of the AAAI Workshop: Artificial Intelligence for Cyber Security*, February, viewed 11 September 2018, <https://www.researchgate.net/publication/287195565_UCO_A_Unified_Cybersecurity_Ontology>.

Theonary, CA & Harrington, AI 2015, *Cyber operations in DoD policy and plans: Issues for Congress*, 5 January, Library of Congress, Congressional Research Service.

Tikk, E, Kasha, K, Runnimeri, K, Kert M, Tali harm AM & Vihul, L 2008, 'Cyber attacks against Georgia: Legal lessons identified', *NATO CCD COE*, Tallinn, EE.

Tolk, A & Smith, B (eds) 2011, 'Command and Control ontology', Editorial, *International Journal of Intelligent Defence Support Systems*, vol. 4, no.3, pp. 209-14.

Undercoffer, J, Joshi, A & Pinkston, J 2003, 'Modeling computer attacks: An ontology for intrusion detection', *Recent Advances in Intrusion Detection (RAID) 2003*, Lecture notes in computer science, vol 2820, G Vigna, C Kruegel & E Jonsson (eds), Springer, Berlin, Heidelberg, DE, pp.113-35.

United States Army 2013, *Joint publication 3-12 (R): Cyberspace operations*, 5 February, viewed 17 September 2018, <<https://nsarchive2.gwu.edu/dc.html?doc=2692126-Document-18>>.

Vrandečić, D 2009, 'Ontology evaluation', *Handbook of ontologies*, 2nd edn, International Handbooks on Information Systems, S Staab, & R Studer (eds), Springer-Verlag, Berlin/Heidelberg, DE, pp. 293-313.

Willems, E 2011, 'Cyber-terrorism in the process industry', *Journal of Computer Fraud & Security*, no. 3, pp.16-9.

Williams, BT 2014, 'The joint force commander's guide to cyberspace operations', *Joint Force Quarterly*, no. 73, vol. 2, pp. 12-19.

Yin, RK 2003, *Case study research: Design and methods*, Applied Social Research Methods Series, vol 5, Sage Publications, Thousand Oaks, CA, US.

Zetter, K 2015, *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*, Crown Publishing Group, New York, NY, US.