Building an Ontology of Cyber Security

Alessandro Oltramari and Lorrie Faith Cranor
CyLab, Carnegie Mellon University
Pittsburgh, USA

Robert J. Walls and Patrick McDaniel
Department of Computer Science
Pennsylvania State University
University Park, USA

***Abstract*—Situation awareness depends on a reliable perception of the environment and comprehension of its semantic structures. In this respect, the cyberspace presents a unique challenge to the situation awareness of users and analysts, since it is a unique combination of human and machine elements, whose complex interactions occur in a global communication network. Accordingly, we outline the underpinnings of an ontology of secure operations in cyberspace. We present the basic architecture of the ontology and provide a modeling example. We make the case for adopting a rigorous semantic model of cyber security to overcome the current limits of the state of the art.**

Keywords— cyber security, ontology, situation awareness, ontology patterns.

I. Introduction

As disclosed by a recent report[1], there has been half a billion cyber security breaches in the first semester of 2014, matching the record set across the entire precedent year. In general, this alarming trend should not surprise when we consider that the bedrock of the Internet is a technological infrastructure built almost 35 years ago for trusted military communications and not for data exchange in the wild (see [1], p.58). The picture gets even worse when considering that the ability to grasp the risk and threats associated with computer networks is averagely poor: recent surveys have actually shown that 65% of the companies victim of intrusion and information theft are usually notified by third parties and that the detection process usually takes 13 months (e.g., see [2], p.10).

Though not exhaustive, such rough statistics at leasts suggests that if the inadequacy of the technological infrastucture is a key aspect to explain the vulnerabilities of networked computer systems, the *human factor* also plays a central role. As proposed in [3], to improve situation awareness of users and security operators, a shift of focus from system to environment level is highly necessary when modeling cyber scenarios: to this end, a full-fledged science of cyber security needs to be founded, whose core principle is *cognizing* the cyberspace as a hybrid framework of interaction between humans and computers, where security and privacy policies play also a crucial role. As stated by [4], this *cognizance* depends on both a reliable perception of the elements of an environment and, most importantly for our work, on the explicit representation of their semantics. Accordingly, the current article presents the underpinnings of an ontology of secure cyber operations: by and large, the concepts and the relationships that structure this semantic model are peculiar to the domain. That is, notions that are suitable for representing security in the physical world cannot be direclty transferred to the cyber environment (e.g., attack attribution [5]). We build upon existing ontologies, expanding them to support novel use cases as needed[2]. Our goal is to use the proposed ontology as basis for improving the situation awareness of cyber defenders, allowing them to make optimal operational decisions given the current environment.

The remaining of the paper is organized as follows: section II will briefly make the case for the adoption of ontologies in the cyber security realm; section III will outline the structure of 'CRATELO', a Three Level Ontology for the Cyber Security Research Alliance program funded by ARL[3], and describe a simple cyber scenario modeled by means of our approach; finally section IV draws preliminary conclusion and outlines an agenda for future research.

II. Related Work

Developing cyber security ontologies is a critical step in the transformation of cyber security to a science. In 2010, the DoD sponsored a study to examine the theory and practice of cyber security, and evaluate whether there are underlying fundamental principles that would make it possible to adopt a more scientific approach. The study team concluded that:
The most important attributes would be the construction of a common language and a set of basic concepts about which the security community can develop a shared understanding. A common language and agreed-upon experimental protocols will facilitate the testing of hypotheses and validation of concepts [6].

The need for controlled vocabularies and ontologies to make progress toward a science of cyber security is recognized in [7] and [8] as well. In this domain, ontologies would include, among other things, the classification of cyber attacks, cyber incidents, malicious and impacted software programs. From our point of view, where the human component of cyber security is crucial, the analysis needs to be expanded to the different roles that attackers, users, defenders and policies play in the context of cyber security, the different tasks that the members of a team are assigned to by the team leader, and the knowledge, skills and abilities needed to fulfill them.

[1] https://www.riskbasedsecurity.com/reports/2014-MidYearDataBreachQuickView.pdf

[2] For instance, exploiting material available in this portal: http://militaryontology.com/cyber-security-ontology.html

[3] http://cra.psu.edu/

There has been little work on ontologies for cyber security and cyber warfare. Within a broader paper, there is a brief discussion of an ontology for DDoS attacks [9] and a general ontology for cyber warfare is discussed in [10]. To the best of our knowledge, Obrst and colleagues [11] provide the most comprehensive description of a cyber ontology architecture, whose vision has actually inspired the work presented in this paper (the scale of the project and its difficulties are also discussed by Dipert in [8]). By and large, efforts that have been made toward developing ontologies of cyber security, even when expressed in OWL, RDF or other XML-based formats, typically do not utilize existing military domain or middle-level ontologies such UCORE-SL[4]. With regard to human users and human computer interaction, the most important step in understanding a complex new domain involves producing accessible terminological definitions and classifications of entities and phenomena, as stressed in [7]. Discussions of cyber warfare and cyber security often begin with the difficulties created by misused terminology (such as characterizing cyber espionage as an attack): in this regard, the Joint Chiefs of Staff created a list of cyber term definitions that has been further developed and improved in a classified version[5]. None of these definitions, however, are structured as an ontology. Likewise, various agencies and corporations (NIST[6], MITRE[7], Verizon[8]) have formulated enumerations of types of malware, vulnerabilities, and exploitations. In particular MITRE, which has been very active in this field, maintains two dictionaries, namely CVE (Common Vulnerabilities and Exposures[9]) and CWE (Common Weakness Enumeration[10]), a classification of attack patterns (CAPEC - Common Attack Pattern Enumeration and Classification[11]), and an XML-structured language to represent cyber threat information (STIX - Structure Threat Information Expression[12]). Regardless of the essential value of these resources, without a "shared semantics" the sprawling definitions they contain are hard to maintain and port into machine-readable formats.

III. A Three-Level Ontology for the Cyber-Security Research Alliance

Top-level ontologies capture generic characteristics of world entities, such as spatial and temporal dimensions, morphology (e.g., parts, edges, sides), qualities (e.g., color, volume, electric charge), etc; because of their inherent generality, they are not suited to model contextual aspects. Nevertheless, it's good practice to describe the fine-grained concepts that constitute a *domain-level* ontology in terms of foundational (or *top-level*) categories, adding core (or *middle-level*) notions to fill contingent conceptual gaps. For instance, an ontology of mineralogy should include notions like "basaltic rock", "texture" and "metamorphic reaction". In order to describe the meaning of those specific concepts, high-level categories such that "object", "quality" and "process" must be employed; the ontology should also define an intermediate notion like "metamorphism", which is common across domains (biology, chemistry, computer science, architecture, etc.), to explain how the different phases, end products, and features of metamorphic reactions are bound together.

Our ontology of cyber security makes no exceptions to the tripartite layering described above: in particular, CRATELO is an ontological framework constituted of a domain ontology of cyber operations (OSCO), designed on the basis of DOLCE top ontology, extended with a middle-level security-related ontology (SECCO), and encoded in OWL-DL. The three levels of CRATELO (schematized in figure 1) currently include 207 classes and 131 relationships (divided into 116 object properties and 15 datatype properties). The expressivity of the ontology is SRIQ, a decidable extension of the description logic SHIN (see [12] for more details).

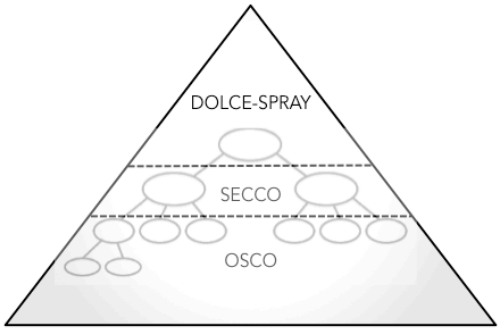

Figure 1: The Schematics of CRATELO

A. *Descriptive Ontology for Linguistic and Cognitive Engineering (DOLCE)*

DOLCE is part of a library of foundational ontologies for the Semantic Web developed under the WonderWeb project (funded by the European Commission[13]). As reflected in the acronym, DOLCE holds a cognitive bias, i.e. aiming at capturing the conceptual primitives underlying natural language and commonsense reasoning [13]. In order to reduce the complexity of the axiomatisation, in the current work we adopt DOLCE-SPRAY[14], a simplified version of DOLCE [14]. The root of the hierarchy of DOLCE-SPRAY is ENTITY, which is defined as the class of anything that is identifiable as an object of experience or thought. The first relevant distinction is among CONCRETE ENTITY, i.e. objects located in definite spatial regions, and ABSTRACT-ENTITY, whose instances don't have spatial properties. CONCRETE-ENTITY is further split in CONTINUANT and OCCURRENT, namely entities without inherent temporal parts (e.g. artifacts, animals, substances) and entities with inherent temporal parts (e.g. events, actions, states) respectively. The basic ontological distinctions are maintained: DOLCE's ENDURANT and PERDURANT match DOLCE-SPRAY's CONTINUANT and OCCURRENT; the core difference comes from merging ABSTRACT and NON–PHYSICAL–ENDURANT categories into DOLCE-SPRAY's ABSTRACT–ENTITY. Among subtypes of

[4] http://www.slideshare.net/BarrySmith3/universal-core-semantic-layer-ucoresl
[5] http://publicintelligence.net/dod-joint-cyber-terms/
[6] http://www.nist.gov/
[7] http://www.mitre.org/
[8] http://www.verizon.com/
[9] https://cve.mitre.org/
[10] http://cwe.mitre.org/
[11] https://capec.mitre.org/
[12] https://stix.mitre.org/language/version1.1.1/
[13] http://wonderweb.man.ac.uk/
[14] Categories are indicated in small caps; relationships in italics. Presenting the axiomatisation of DOLCE-SPRAY is out of scope in this paper.

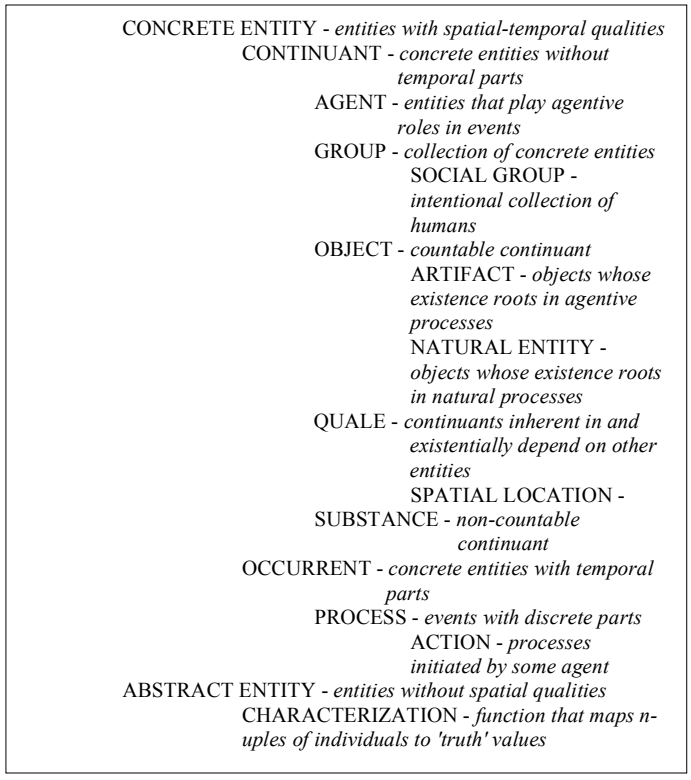

Figure 2: DOLCE-SPRAY backbone taxonomy

this category, CHARACTERIZATION is defined as a mapping of n-uples of individuals to truth-values. Individuals belonging to CHARACTERIZATION can be regarded to as "reified concepts" (e.g. "manufactured object"), and the irreflexive, antisymmetric relation CHARACTERIZE associates them with the objects they denote ("a collection of vintage shoes"). Among the relevant sub-types of CHARACTERIZATION we can find: ROLE, i.e. the classification of an entity according to a given context or perspective; PLAN, namely the generic description of an action (such as "the disassembly of a 9mm"); TASK, that is a representation of the specific steps that are needed to execute an ACTION according to a PLAN (e.g. "removing the magazine", "pull back the slide"); REQUIREMENT, whose instances can be seen as the preconditions that need to be satisfied as part of a PLAN (e.g. "the weapon must be clear before proceeding"). The branch of the DOLCE-SPRAY rooted on CHARACTERIZATION distills the extensions introduced in [15]. An overview of DOLCE-SPRAY's backbone taxonomy is represented in figure 2.

B. Security Core Ontology (SECCO)

In order to extend DOLCE-SPRAY for characterizing security, we designed a minimal set of ontological concepts. In particular, an entity is a THREAT ϕ for an ASSET α *valued by* a STAKEHOLDER σ and *protected by* a DEFENDER δ, if and only if ϕ can be *used by* an ATTACKER κ to *exploit* a VULNERABILITY ϖ of α in an ATTACK τ[15]. To avoid ϕ, a specific collection of SECURITY-REQUIREMENTs υs need to *be satisfied by* α. When τ is launched, δ has to perform a suitable OPERATION o and *deploy* COUNTERMEASUREs χs to proactively defend α; o is carried out on the basis of a MISSION-PLAN π whose sequence of MISSION-TASKs ξs needs to *be executed in* o[16]. In order to delineate π, δ needs also to preemptively *assess* the RISK ρ *associated to* τ (datatype properties can be used to represent ρ as a parameterization of the expected losses, probabilities of attack, etc.).

The list of class-inclusions below (1-6) denotes the alignment between SECCO and DOLCE-SPRAY's main categories. Note that the multiple inheritance in (1-3) is based on 'rigidity', a meta-class defined in [16]: in summary, we can say that 'agent' is a rigid class because every entity that is classified by this notion fulfills some necessary requisites; on the contrary, 'role' is an anti-rigid class because an entity can be conceived as an attacker only on some situations. To put it in other words: we, as persons, will be always agents, no matter what we do; but only if we attack someone or something, we can be considered both agents and attackers.

$$ATTACKER, DEFENDER, STAKEHOLDER \sqsubseteq AGENT, ROLE \quad (1)$$
$$ATTACK, OPERATION \sqsubseteq ACTION, ROLE \quad (2)$$
$$ASSET, THREAT, COUNTERMEASURE \sqsubseteq OBJECT, ROLE \quad (3)$$
$$RISK, VULNERABILITY \sqsubseteq QUALE \quad (4)$$
$$SECURITY-REQUIREMENT \sqsubseteq REQUIREMENT \quad (5)$$
$$MISSION-PLAN \sqsubseteq PLAN \quad (6)$$
$$MISSION-TASK \sqsubseteq TASK \quad (7)$$

As this semantic framework suggests, SECCO's categories are positioned at a too coarse-level of granularity to capture the details of domain-specific scenarios: properties like THREAT, VULNERABILITY, ATTACK, COUNTERMEASURE, ASSET are orthogonal to different domains and, in virtue of this, they can be predicated of a broad spectrum of things: for instance, infections are a threat to the human body, Stuxnet is a threat to PLCs, the impact of large asteroids on the Earth's surface is a threat to the survival of organic life forms, dictatorship is a threat to civil liberties, and so and so forth. Though there seems to be a consensus in the literature on the core ontological concepts of security (see [17] and [18]), the minimal set presented here has been occasionally expanded along alternate directions. For instance, Fenz and Ekelhart [19] introduce the concept of CONTROL, by means of which stakeholders implement suitable countermeasures to mitigate known vulnerabilities[17] of assets. A POLICY, in this context, is defined as a regulatory or organizational form of control. [19] also outlines a taxonomy of assets, distinguishing TANGIBLE (wallet) from INTANGIBLE ones (credit card information), where the former can be furthermore split into MOVABLE (e.g., car, jewelry) and UNMOVABLE (e.g., house, land of property). Interestingly enough, Fenz and Ekelhart reify the procedure of assessing a risk into the concept of RATING, whose attributes can be expressed qualitatively (e.g. in Likert scale – high, medium and low) or quantitatively (measuring the probability of a risk). Avižienis and colleagues present a comprehensive

[15] Note that δ and σ may or may not coincide: in the second case, the latter needs to delegate the former to act in her behalf. The notion of delegation (and trust) in agent ontologies has been extensively studied by [26], but it's currently not included in CRATELO.

[16] o can be a single ACTION or a complex set of interconnected actions.

[17] In cyber security, exploitations of unknown vulnerabilities correspond to the so-called Zero-Day Attacks.

analysis of security where the notion of FAULT is introduced to denote an interruption of the services delivered by a given system in the environment [20]. Though a middle-level ontology of security can be optionally extended beyond the minimal set of concepts outlined at the beginning of this section, what is original in our approach is the characterization of SECCO's security primitives using DOLCE-SPRAY.

C. Ontologies of Secure Cyber Operations (OSCO)

One of the major cyber security problems for government and corporations is the widespread "operational chaos" experienced by analysts, as Michael Susong has recently called the phenomenon of "having too many alarms (false positives) in a network, not enough trained people to deal with them, and a consequent poor prioritization of risks and countermeasures" [18]. In this regard, the objective of an ontology of cyber security is to shape that chaos into framework of meaningful and reusable chunks of knowledge, turning the operational disarray into a systematic model by means of which analysts can increase their situation awareness of cyber operations. As mentioned before (see section 1), the key to this augmented *cognizance* relies on a consistent assessment of the situation and on a comprehensive understanding of its elements at the semantic level. But how is a cyber operation usually defined? In a document released in 2010, the Joint Chiefs of Staff describes a "cyberspace operation" as the "employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid" [21]. Drawing on this broad definition, and utilizing the concepts introduced in sections A and B, we represent a CYBER-OPERATION ψ as an OPERATION *executed by* a CYBER-OPERATOR φ, who plays the role of DEFENDER in the context of a CYBER-ATTACK θ (7-8). For the sake of this article, we will limit ourselves to provide an example of a cyber operation with CRATELO, since the development of a full-scale domain ontology is currently underway within our project).

$$CYBER-OPERATION \sqsubseteq OPERATION \quad (7)$$

$$CYBER-OPERATOR \sqsubseteq DEFENDER \quad (8)$$

$$CYBER-ATTACK \sqsubseteq ATTACK \quad (9)$$

1) Modeling "RETRIEVE-FILE-SECURELY" with CRATELO

Figure 3 represents CRATELO's classes and relationships used to model the RETRIEVE-FILE-SECURELY scenario. For limits of visualization, the diagram covers only the most salient notions involved in this cyber operation.

In order to retrieve a file without exposing a computer system – and possibly an entire network – to cyber threats, some specific security requirements need to be fulfilled while carrying out that operation. In particular, as it is also the case for other kinds of CYBER-OPERATION, RETRIEVE-FILE-SECURELY must occur over a secure channel of a network, from authenticated computer(s) and through authorized server(s). By and large, abiding to these security requirements while executing the mission-tasks should lead to mission accomplishment. The composite RETRIEVE-FILE-SECURELY-TASK can be further divided into simpler temporally-structured and logically-connected subtasks. Accordingly, a request for a file can be sent to an authenticated server only after locating the desired file in the network; the inspection of the file can trivially occur only once the file has been obtained; and so on and so forth. In CRATELO we can express these basic temporal constraints by means of the foundational layer: in fact, DOLCE includes an adaptation of Allen's axioms [22], which are considered as a powerful logical theory for temporal representation and reasoning (the formalization of these axioms has also been maintained in DOLCE-SPRAY). Moreover, if malware is detected, the file has to be removed from the host: the deployment of this preventive countermeasure aims at avoiding a disruption of the isolated computer node and a cyber attack to the network it belongs to. This countermeasure can be expressed as a conditional rule formalized in CRATELO by using an additional modeling apparatus, i.e. the Semantic Web Rule Language (SWRL)[19], which extends OWL-DL axioms. By including rule-based mechanisms in CRATELO we also comply with the core requisites described in [11] of a full-fledged cyber ontology architecture.

As the example reveals, one of the key design principles underlying CRATELO is to separate the temporal dynamics of cyber operations from the abstract generalizations used to describe them, i.e., plans, tasks, requirements. This approach consents to model a cyber operation as an 'ontology pattern' grounded on the top level dyad OCCURRENT-CHARACTERIZATION and, most importantly, unfolded by the middle-level tetrad [CYBER-OPERATION]-MISSION-PLAN-[SECURITY-REQUIREMENT]. In recent years, 'ontology patterns' have become an important instrument in the area of conceptual modeling and ontology engineering [23]: the rationale, as our work suggests, is to identify some minimal knowledge structures to be used as the building blocks for modeling a problem or a scenario in an ontology. This methodology is also ideal from a reasoning point of view. For instance, in [24] the authors state that "mission activities are tasks focused on answering mission questions" (where the latters can be seen as partially overlapping the notion of security requirements): but an ontology that fails to discriminate "activities" from "tasks" would likely be affected in its inference capabilities, in the degree that reasoning over tasks that have not been executed yet – i.e. that are not activities – would not be supported. It's not difficult to imagine the circumstances where this limit can become a serious drawback for the situation awareness of a cyber analyst: mental simulation is commonly adopted by humans to foresee the outcomes of an action before performing it [25], and a semantic model where mission activities and tasks are conceptually viewed as the same entity precludes that, and might eventually result into pervasive logical inconsistencies, if the ambiguity is not somehow constrained. On the contrary, applying CRATELO's ontology-pattern allows us to specify cyber operations at a suitable level of conceptual granularity.

[18] Dr. Micheal Susong is an Intelligence Subject Matter Expert affliated to iSIGHT Partners; he gave an invited talk at Carnegie Mellon University on September 8th, 2014.

[19] http://www.w3.org/Submission/SWRL/

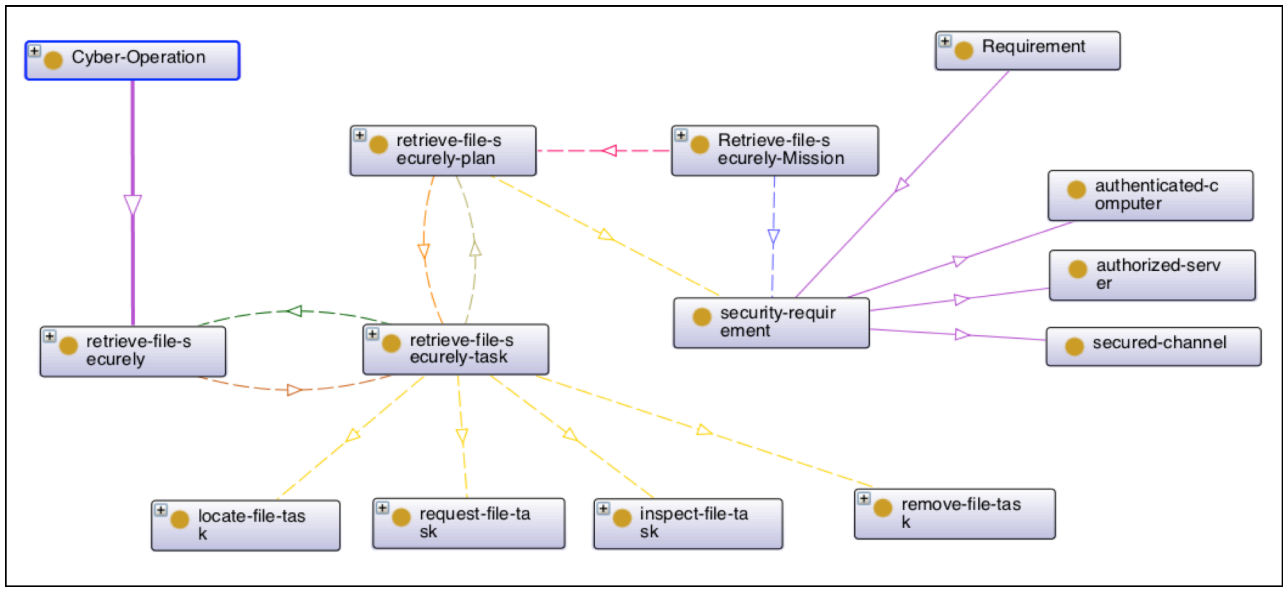

Figure 3 – A visualization of the "Retrieve-file-securely" cyber operation modeled in CRATELO. Legend of the arc types: 'has subclass' (purple); 'is executed in' (green); 'executes' (brown); 'has part' (yellow); 'defines task' (orange); 'is defined in task' (ochre); 'satisfies (all)' (fuchsia); 'satisfies (some)' (electric blue).

IV. Conclusions And Future Work

Notwithstanding the proliferation of taxonomies, dictionaries, glossaries, and terminologies of the cyber landscape, building a comprehensive model of this domain remains a major objective for the community of reference, that includes government agencies, private organizations, researchers and intelligence professionals. There are multiple reasons behind the discrepancy between demand and supply of semantic models of cyber security. Although we can't thoroughly address this topic here, we are firmly convinced that a great part of the problem is the lack of balance between the 'vertical' and the 'horizontal' directions of the effort. From one side, state of the art consists of several classifications of the domain, as argued in section II: these efforts typically yields rich catalogs of cyber attacks, exploits and vulnerabilities. On the other side, a rigorous conceptual analysis of the entities and relationships that are encompassed by different cyber scenarios would also be needed, but few work has been done on this horizontal dimension (if we exclude the ongoing MITRE initiative described by Leo Obrst and colleagues in [11]). In this paper we placed ourselves on the second perspective: instead of presenting "yet another" catalog of cyber notions, an endeavor that remains however of undisputable relevance, we decided to explore in depth the semantic space of cyber operations. Our investigation addresses cyber operations as complex entities where the human factor is as important as the technological spectrum: our ontological analysis is grounded on a bedrock of foundational concepts and reaches the domain of cyber operations through an intermediate layer where core notions are defined.

Future work will focus on the following research steps:

- to focus on the ontological analysis of risk;
- to populate the domain ontology with a large set of cyber operations documented in the literature and learned from real-world case studies;
- to design and customize a methodology for ontology validation based on "competency questions" submitted to domain experts (along to what has been proposed in [19]);
- to run cyber warfare simulations within military exercises, collecting data to be modeled with CRATELO;
- to study ontology mappings beteween CRATELO and other semantic models (e.g. MITRE's Cyber Ontology Architecture), ensuring interoperability and reusability of the resource.

We are aware of the challenges ahead of us in pursuing this research agenda, which would usually be very difficult to implement. Nevertheless, we're also persuaded that, in the broad vision framed by the ARL Cyber Security Collaborative Research Alliance, what we have described here illustrates a realistic work plan and a necessary step toward the foundation of a science of cyber security.

Acknowledgments

Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

REFERENCES

[1] P. and Lowther, A. B. Yannakogeorgos, "The Prospects of Cyber Deterrence: American Sponsorships of Global Norms," in *Conflict and Cooperation in Cyberspace*.: Taylor&Francis, 2013, pp. 49-77.

[2] L. Mattice, "Taming the "21st Century's Wild West" of Cyberspace?," in *Conflict and Cooperation in Cyberspace*.: Taylor&Francis, 2013, pp. 9-12.

[3] P., Rivera, B., Swami, A. McDaniel, "Toward a Science of Secure Environments," *Security and Privacy*, vol. 12, no. 4, pp. 68-70, July/August 2014.

[4] M.R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, vol. 37, no. 1, pp. 32-64, 1995.

[5] H. Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, vol. 6, no. 3, pp. 46-70, Fall 2012.

[6] The MITRE Corporation, "Science of Cyber-Security," The MITRE Corporation, McLean, VA, Technical 2010.

[7] D. A. Mundie and D. M. McIntire, "The MAL: A Malware Analysis Lexicon," CERT® Program - Carnegie Mellon University , Technical 2013.

[8] R. Dipert, "The Essential Features of an Ontology for Cyberwarfare," in *Conflict and Cooperation in Cyberspace - The Challenge to National Security*, Panayotis A Yannakogeorgos and A. B. Lowther, Eds.: Taylor & Francis, 2013, pp. 35-48.

[9] I. Kotenko, "Agent-Based modeling and simulation of cyber-warfare between malefactors and security agents in internet ," in *19th European Conference on Modeling and Simulation*, 2005.

[10] A., Buchanan, L., Goodall, J. & Walczak, P. D'Amico. (2009) Mission impact of cyber events: Scenarios and ontology to express the relationship between cyber assets. [Online]. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA517410

[11] L., Chase, P., & Markeloff, R. Obrst, "Developing an ontology of the cyber security domain," in *Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security*, 2012, pp. 49-56).

[12] I., Kutz, O., Sattler, U. Horrocks, "The Irresistible SRIQ ," in *OWLED '05 - "OWL: Experiences and Directions"*, vol. 188, Galway, 2005.

[13] C., Borgo, S., Gangemi, A., Guarino, N., Oltramari, Schneider, L. A. Masolo, "The WonderWeb Library of Foundational Ontologies and the DOLCE ontology," Laboratory For Applied Ontology, ISTC-CNR, Technical Report 2002.

[14] Vetere G., Jezek E., Chiari I., Zanzotto F.M., Nissim M., Gangemi A. Oltramari A., "Senso Comune: A Collaborative Knowledge Resource for Italian," in *The People's Web Meets NLP: Collaboratively Constructed Language Resources.*: Springer Verlag, 2013, pp. 45-67.

[15] A., Mika, P. Gangemi, "Understanding the Semantic Web through Descriptions and Situations," in *On The Move to Meaningful Internet Systems - Lecture Notes in Computer Science*. Berlin-Heidelberg: Springer, 2003, vol. 2888, pp. 689-706.

[16] Welty, C. Guarino, N. "Evaluating ontological decisions with OntoClean," *Communications of the ACM 45 (2), 61-65*, vol. 45, no. 2, pp. 61-65, 2002.

[17] C. Salinesi, I., Wattiau, I. A. Souag, "Ontologies for Security Requirements: A Literature Survey and Classification," in *Advanced Information Systems Engineering Workshops*, vol. 112, 2012, pp. 61-69.

[18] M. Schumacher, "Toward a Security Core Ontology," in *Security Engineering with Patterns*. Berling-Heidelberg: Springer-Verlag, 2003, pp. 87-96.

[19] S., Ekelhart, A. Fenz, "Formalizing Information Security Knowledge," in *th International Symposium on Information, Computer, and Communications Security (ASIACCS '09)*, New York, pp. 183-194.

[20] A., Laprie, J., Randell, B., Landwehr, C. Avizienis, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11-33, January-March 2004.

[21] Joint Staff Department of Defense. Joint Terminology for Cyber Operations. [Online]. http://afri.au.af.mil/cyber/Docs/panel1/Cyber_Lexicon.pdf

[22] J.F. Allen, "An interval based representation of temporal knowledge," in *7th International Joint Conference on Artificial Intelligence (IJCAI)*, vol. 1, Vancouver, 1983, pp. 221–226.

[23] A. and Presutti, V. Gangemi, "Ontology design patterns," in *Handbook on Ontologies*.: Springer , 2009, pp. 221-244.

[24] T.I., Mayron, L.M., Smith, W.B., Knepper, M.M., Reg, I., Fox, K.L. Morris, "A perceptually-relevant model-based cyber threat prediction method for enterprise mission assurance," in *IEEE Multi-disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, Miami Beach, 2011, pp. 60-65.

[25] S.E., Pham L.B., Rivkin I.D., Armor D.A. Taylor, "Harnessing the imagination. Mental simulation, self-regulation, and coping.," *American Psychologist* , vol. 53, no. 4, pp. 429-439, Apr 1998.

[26] C., Falcone, R. Castelfranchi, *Trust Theory: A Socio-Cognitive and Computational Model*.: Wileyand, 2010.