Proceedings of the 2015 Winter Simulation Conference
L. Yilmaz, W. K. V. Chan, I. Moon, T. M. K. Roeder, C. Macal, and M. D. Rossetti, eds.

SYSTEM OF SYSTEMS CYBER EFFECTS SIMULATION ONTOLOGY

David Ormrod

Australian Center for Cyber Security
University of New South Wales at the
Australian Defense Force Academy
Australian Capital Territory, AUSTRALIA

Benjamin Turnbull

Australian Center for Cyber Security
University of New South Wales at the
Australian Defense Force Academy
Australian Capital Territory, AUSTRALIA

Kent O'Sullivan

Australian Center for Cyber Security
University of New South Wales at the
Australian Defense Force Academy
Australian Capital Territory, AUSTRALIA

ABSTRACT

This paper outlines the requirements for a series of ontologies necessary to provide a meaningful answer to the question: ***How do we model and simulate the System of Systems effects of a cyber attack on an organization or military unit?*** This work provides the data model specification for a simulation to answer this question by explaining the required domains of knowledge. We introduce mechanisms to federate these domains, and then provide an exemplar use-case to contextualize one type of scenario the model must be capable of representing within a simulation environment. The model demonstrates the granularity necessary for the modeling and simulation of a SoS effect of a cyber attack on an organization or military unit.

DISCLAIMER

The views expressed are the authors' and not necessarily those of the Australian Army or the Department of Defence. The Commonwealth of Australia will not be legally responsible in contract, tort or otherwise for any statement made in this publication.

1 INTRODUCTION

This paper describes an ontology that answers the question: ***How do we model and simulate the System-of-Systems (SoS) effects of a cyber attack on an organization or military unit?*** The question resulted from a desire to develop a simulation capable of modeling the broader, organizational consequences resulting from a cyber attack.

It is not a simple task to model or simulate the key factors that can determine the effects of a cyber attack. If the model is too simplistic, it will not be trusted nor will it accurately portray the factors and their influence on the system. This work seeks to solve this issue through the development of multiple ontologies encompassing several disparate domains of discourse. Each of these domains represents a key driver in how a cyber attack occurs, or the potential effect a cyber incident can have in an area. Additionally, each of these ontologies should be independently functional and comprehensive. These ontologies are then federated through a novel approach for our intended use-case; a simulation for the express purpose of modeling cyber attack impact. The scope of the paper includes a brief description of the problem space, a review of the highest levels of the ontology, an introduction to the mechanisms we are using to federate disparate

ontologies, and the introduction of an exemplar use case in a specific organizational context. In this paper we are not providing an exhaustive explanation of the ontology. Rather, we provide an overview of the domains, a review of their interactions and describe the underpinning ontological approach in an effort to further the state of the art and provide context for future work.

2 PROBLEM SPACE

The Cyber Security Research Roadmap (Maughan 2009) identified the composition of cyber networks as a contemporary risk, lacking predictable confidence. Systems evolve in order to be relevant to changing environments and user requirements, but this evolution makes the system weaker from a security perspective and less trustworthy. "As a result, today the security of a system of systems may be drastically less than that of most of its components" (Maughan 2009, p2). Information security does not occur in a static environment, which creates opportunities for attackers. The implications of cyber attacks on military systems has been discussed extensively (Arbuthnot 2013, Liff 2012, Carr 2010, Leed 2013). The loss of integrity can lead to deception, the loss of confidentiality can compromise battle plans, and the loss of availability can lead to denial of service and compromised situational awareness (Schramm and Gaver 2013). A cyber attack by an adversary on the confidentiality of networked command and control systems could provide visibility of dispositions and plans (Nesteruk 2009). Despite these risks, many decision makers are unable to access quantitative data to make informed decisions to optimize system protection or support policy decisions for network defense.

SoS are tightly coupled systems that feature independent aspects, emergent behavior and evolutionary development (Sage and Cuppan 2001). They are evolving environments that are highly complex (Efatmaneshnik and Ryan, 2014). Human factors have been demonstrated as critical to understanding military SoS (Jackson and Keys 1984). Examples include the shooting down of Iran Air Flight 655 (Cannon-Bowers and Salas 1998) and the failure of the German military to secure ciphers (Ratcliff 2006). Human factors are difficult to represent and are therefore underrepresented in existing models. However, removing the human from a model seeks simplicity whilst ignoring the objective of combined arms maneuver in combat: "…to break the enemy's will through relentless and continuous pressure" (US Department of the Army 2012, p28). Information systems in the military environment are a component of the SoS, intended to enable the destruction of the enemy's will through command and control (Van Creveld 1985).

Ontologies specify the content of shared knowledge within knowledge based systems, as "an explicit specification of a conceptualization" (Gruber 1993, p1). Efforts to model and trace the propagation of cyber effects across multiple distinct domains requires a specific ontology. Abstraction is necessary to allow for efficient computation and to reduce complexity. Simplicity and abstraction must be balanced with the need for a practical tool set capable of reflecting the complexity of the SoS. The ontology must be capable of using common objects as well as the ability to model effects from one discipline to another. The ontology and models must be flexible and robust to permit reuse and extension. An artefact capable of modeling the SoS effects of a cyber attack would support the development of robust risk assessments, business continuity plans and organizational resilience measures.

3 CURRENT WORK IN THE AREA

Cyber impacts are described in many government reports as qualitative outcomes (US Department of Defense 2013b, Amoroso 2012, Frankel 2000). In contrast, cyber impact literature tends to focus on the technical aspects without adequately describing the human aspects of the problem space. Increased coupling of systems increases the dependence between systems (Wilson, 2007) and the likelihood of emergent and unintended consequences (Weber and Khademian 2008). The barriers to simulating cyber impact have been discussed by Cohen (1999). He proposed variable granularity, using an iterative development process reinforced with validation activities to compare the simulation of human factors and cyber impacts with

real world results. His model is difficult to reuse against specific network vulnerabilities or network defense strategies. It would require extension to model human factors in a military environment.

Konstantinia and Andrew (2013) have developed an impact assessment model based on Socio-Technical-System (STS) theory that seeks to incorporate human factors in the consideration of information system risk. The framework they present consists of responsibilities, roles, tasks, obligations and commitments between agents with responsibility dependency trees. Human factors, whilst discussed, are not reflected in detail and are flagged for future work (Charitoudi and Blyth 2014). The model has utility but it seems to lack extensibility based on the limited examples available.

Cyber-ARGUS models the network and mission separately, before mapping services and nodes to form a Mission Network Graph (Costa, Hieb, and de Barros Barreto 2014). This approach does not appear to incorporate any human factors. Related research into defensive cyber damage and mission impact methodologies include Bernier, LeBlanc, and Morton (2012), Fortson Jr (2007) and Argauer (2007). The impact of cyber attacks on the decision making process is discussed in Cayirci and Ghergherehchi (2011). The cyber impact models reviewed by the authors provide scant detail on the relationships within and between domains.

The Future Situation and Impact Awareness (FuSIA) system is designed to model the state of a network; to show hosts, routing and vulnerabilities (Holsopple and Yang 2008). The goal is a security and cyber situational awareness tool. The primary data model used by FuSIA is an ontology named 'Virtual Terrain'. The information on Virtual Terrain is brief (Holsopple, Yang, and Sudit 2015), but its primary purpose is to model entities, configuration information, vulnerabilities and events. There is, however, no indication of any temporal aspect in FuSIA or Virtual Terrain. Without access to the Virtual Terrain ontology we cannot analyze how it performs against its original intentions nor can we adapt it to our own use-cases.

CAMUS seeks to determine the criticality of cyber assets to projects (D'Amico et al. 2009, Goodall, D'Amico, and Kopylec 2009). The main data model used for CAMUS is an ontological data store. CAMUS maps assets, projects, sub-tasks, and people with links. Whist CAMUS is a situational awareness tool for the cyber realm, the tool is not all-encompassing. The CAMUS ontology is designed to meet a specific goal. It has limited extensibility. CAMUS was later expanded (Watters et al. 2009) to include concepts surrounding confidentiality, sensitivity and the implications to a mission if specific nodes (cyber assets) were impacted (Musman and Agbolosu-Amison 2014, Buchanan et al. 2012). The use-case for CAMUS is quite simplistic in nature and there are few available to adapt for a different purpose. The lack of public ontology and model development makes reuse difficult.

Musman et al. (2011) proposed a Cyber Mission Impact Assessment (CMIA) where IT activities link to mission process activities (Musman and Agbolosu-Amison 2014). The examples are generally denial of service attacks with a temporal mission impact. CMIA features a mission impact analysis seemingly absent in many other models. However a focus on activities appears to capture directed attacks only, such as denial of service, without modeling the vulnerabilities leading to network infection or a loss of data integrity.

Sol (Bradshaw et al. 2012) is another project using an agent-based framework for cyber situational awareness. The implementation of the process is relatively nascent. This paper has no discussion about any intermediate data model used, although the system makes use of the KAoS policy services framework.

CyMRisk is an approach for computing mission risk due to cyber attacks (Llanso and Klatt 2014). The model substitutes likelihood with level of effort. In the SoS context a high level of effort for an attack by a nation state may not align with a low risk likelihood. CyMRisk has a strong technical focus rather than analyzing impact at the SoS level or considering human factors extensively.

The Cyber Incident Mission Impact Assessment (CIMIA) process called for a paradigm shift in methods for mission impact assessment (Grimaila, Fortson, and Sutton 2009). This work argued that decision makers had few means to assess valuable information on cyber networks to aid their decision making. However, CIMIA did not appear to result in an openly available solution.

The cyber attack and defense process has been discussed by Kotenko (2010) as a discrete-event, multi-agent and packet-level simulation of network protocols. The use of a cyber attack has been studied by other authors such as Costantini (2007) and Grimaila and Badiru (2011). These models generally consider the

intersystem effects of a successful cyber attack within a very narrow and technical scope. Kundur et al. (2011) has modeled the impact of cyber attacks using directed graphs and cause-effect relations to describe attacks on the smart grid. Other studies in the electrical, oil and gas industries that are focused on modeling cyber attacks include Negrete-Pincetic, Yoshida, and Gross (2009), Vieira, Houmb, and Insua (2014), Boyer (2011) and Amin (2011).

Distinct from the modeling of cyber impacts is the modeling of combat effects. In many cases, combat simulations include a networking and communications capability as well as a rendering of situational awareness by agents (Tolk 2012). Agent based combat simulation models include ISAAC and the Project Albert product (Ilachinski 2004), MANA (Lauren and Stephen 2002) and CROCADILE (Barlow and Easton 2002). Other agent based simulations with a more physics based approach include JANUS (Berzins 1999) and OneSAF (Wittman Jr and Surdu 2005). A review of combat simulations has been provided by a number of authors, including Bharathy, Yilmaz, and Tolk (2012) and Straver, Vincent, and Fournier (2006). Despite the diversity of combat simulations, the CESO ontology provides a novel approach to modeling cyber attack effects in a military combat environment, not evident in the available combat simulations. The possibility of federation and the means of representing combat within the CESO is under review.

We have sought to apply the advice of Tolk et al. (2012, p2353) in the development of the CESO and "…move from traditional positivism, as represented by Newtonian physics, towards modernity and post-modernity approaches". Building a model sufficiently detailed to allow the observation of effects propagation but simple enough to avoid becoming inordinately complex is challenging (Robinson 2009, Robinson et al. 2013, Lucas and Sanchez 2003). The requirement for this balance is to enable us to see the impact that changes to the attributes of specific assets in the model have on the system as a whole, akin to the concept of microscopic changes leading to macroscopic effects in agent-based models described by Epstein (1999). Such an approach has been discussed extensively in Kott, Wang, and Erbacher (2014). the CESO abstracts the problem space into separate domains, each represented by their own ontology.

4 DOMAINS AND ONTOLOGIES

From the literature, we have determined that there is no existing ontology or model that describes the same domains of knowledge for the same purposes and at the same granularity as proposed within this paper. The CESO is an ontological ecosystem modeling the disparate domains of knowledge required to understand cyber attacks, cyber defenses and to observe their impact on organizational or military endeavors. The CESO is a hierarchical collection of interacting ontologies. Figure 1 represents the highest level of abstraction, divided into two layers, the Shared Attributes layer and the Domain layer.

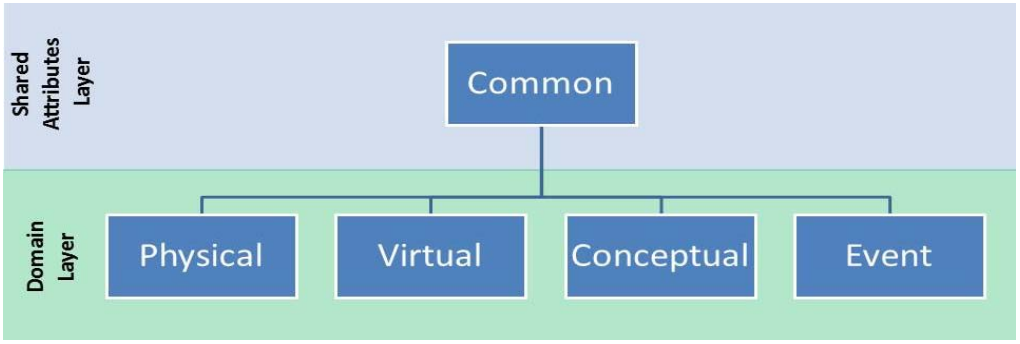

Figure 1 - The Cyber Effects Simulation Ontology (CESO)

The Shared Attributes layer is common to all things within The CESO and holds within it all of the common attributes used by all abstractions. Each domain within the ontology shares these common attributes. These have been termed 'common'. These attributes include a unique instance identifier,

universal concepts such as time, and relationship metaproperties related to inference, which is discussed further in section 5.1. The Domain layer is comprised of four domains, each of which allows event modeling and effect propagation through a network of connected nodes. The Virtual, Physical, Conceptual and Event Domains allow elements of the model to be distinguished and interactions across domains to be mapped. Each domain is discussed below.

4.1 The Physical Domain

The Physical Domain encompasses all of the 'tangibles' of the model. In this ontology, these 'tangibles' are abstracted as 'physical assets' in recognition of shared attributes of all physical objects such as the ability to be seen, touched and to be interacted with. Physical assets have different configurations depending on their purpose and how they have been ordered or created. For example a physical asset could be an infantry soldier, a tank, a computer work station or the cables physically connecting computers together.

4.2 The Virtual Domain

The Virtual Domain is commonly conceptualized as 'cyberspace' It is a combination of the 'logical' and 'cyber-persona' layers in the United States Joint Cyber Operations Doctrine (US Department of Defense 2013a). The ontology combines these layers as the distinction is not necessary at the highest level of abstraction. The virtual domain contains 'virtual assets' that are each separately defined by their configuration. Examples of 'virtual assets' include a user account, firewall, installed operating system, email message or software vulnerability. The cyber-persona also exists within the virtual domain, as a representation of a user.

4.3 The Conceptual Domain

The Conceptual Domain encompasses all of the enabling activities of the model that allow it to function in a meaningful way. This is not to be confused with the type of 'conceptual model' discussed in Robinson (2008). The conceptual domain within this ontology has two key functions: (1) the creation of 'organizations', and (2) the control of processes. Logical grouping of assets creates organizations or architectures. Relationships are made between nodes representing permissions and allegiance. Processes define all of the abstract ideas like missions, situational awareness and decision processes. Missions are the goals and objectives of the organization or asset. Situational awareness is the information available to the organization or asset for decision making. This will be bounded by the information transmitted through the network, availability at nodes and factors such as trust, reliability and personality. The decision process includes situational awareness (which will vary across the network) and human factors.

4.4 The Event Domain

The Event Domain is where the 'activity' occurs. Importantly, this domain enables the intra and inter-domain interactions between the physical and virtual – the vital element in order to model how the impact of an event in one domain propagates across the others. The event domain will log the changes in state of the assets of the physical and virtual domain and reconcile this with the conceptual domain to create a narrative of occurrences.

5 LINKING DISPARATE ONTOLOGIES

The next section discusses the performance of logical reasoning between disparate ontologies. One of the issues with the creation of multiple ontologies for either a single use-case or for interacting systems is how to connect disparate knowledge representations. This work takes two approaches to link the disparate ontologies; the identification of common objects and the development of an inference layer.

5.1 Developing Ontologies with Common Objects

The first mechanism employed to link disparate domains is to use common objects as reference points. Mapping common object types across domains allows for more efficient modeling of connections between domains. For example, a computer crosses multiple domains. In the Virtual domain, the purpose of a Computer object is to depict the data it holds, software, interactions across networks and configuration options. In the Physical domain, Computer is a subclass of asset, and has properties related to asset numbers, physical location and custodian. In the Conceptual domain, the Computer belongs to a specified architecture and an organization. In the Event domain, the same Computer object is modeled through its various changes in state. A computer may be on or off, logged in through a user profile or compromised. The same object has several views. These common concepts bridge otherwise independent ontologies. For maximum reuse independent ontologies are required. Multiple use-cases will involve only one domain. Modeling the effects of cyber security breaches on missions and processes requires interrelated ontologies. Linking common objects limits dependencies between ontologies while still allowing interconnectivity. This approach allows integration of existing ontologies into the model.

5.2 Development of an Inference Layer

The use of common objects alone is not enough. One of the primary requirements of the proposed interlinked data model is the ability to model effects from one discipline in another. For example, if the data model shows that a particular computer has been compromised and its availability has been affected, that same computer instance that is a prerequisite asset in one or more processes is not available. From this the impact on specific business processes can be determined. Technically, this search could be performed every time it is necessary to determine whether a business process has been compromised, but the ongoing complexity is not only resource intensive, it is also difficult to conceptualize.

Instead an extension to the Common ontology we term the *inference layer* is used. The inference layer details a namespace and a form of relationship that is inference-only. The inference layer has the primary purpose of modeling the effects of data at one domain across into another. Inference relationships can only be created by a few select simulation components, as they contravene the modeling tenet that data should only be represented in a single, consistent manner. The inference layer is primarily for agents and system components to search. Periodically, these relationships can be refreshed or removed as the underlying rules that govern them change. The agents or system components that create inferred relationships do so based on a series of Modus ponens/tolens ('if this, then that') rules. In this respect the inference layer is analogous to a read-cache on the database. It provides a level of convenience. Provided the inference layer is backed by an understanding of when to create and destroy inferred relationships, it is an effective approach to model the inferred effects between domains.

6 EXAMPLE USE CASE

The basic use case for an artillery fire mission in a land combat environment is depicted in figure 2. A fire mission occurs when a Joint Fire Team (JFT) requests artillery support. In this simplified example, a JFT actor sends a Call For Fire message. A Joint Fire Coordination Centre (JFCC) subsequently conducts safety checks, confirms the priority of a mission and approves the request. The JFCC also manages a fire mission queue of approved requests ranked by priority. An Artillery Battery actor is then assigned a fire mission by the JFCC from the queue. The battery fires a salvo to complete the fire mission.

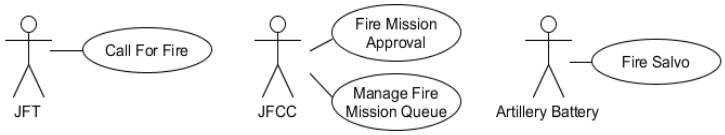

Figure 2 - Fire Mission Business Process Use Cases

Figure 3 provides an example of the Fire Mission Use Case across the four domains. The following terms will be used as a key to describe the interaction of the following domains as the business process is executed: (P) = Physical, (V) = Virtual, (C) = Conceptual and (E) = Effect. Please note that this example is not exhaustive. A few components (such as feedback from the JFT of effects on target, damage modeling and the detail of virtual or network interactions) have not been included in the interests of space.

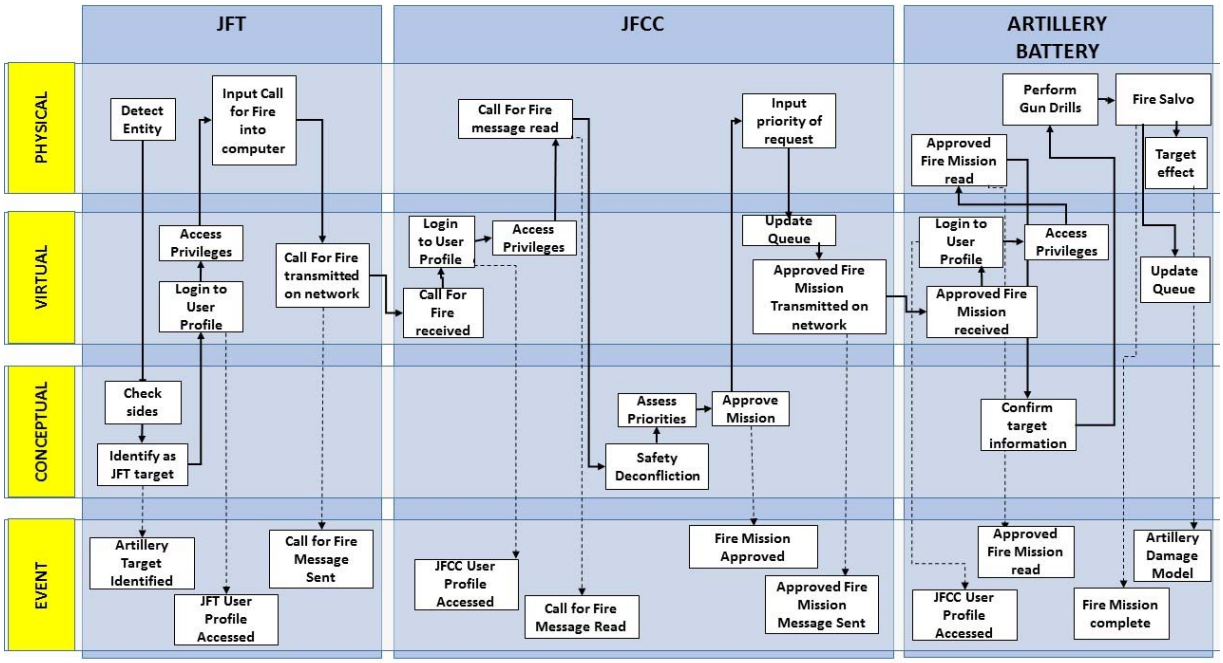

Figure 3 - Fire Mission Cross Domain Process

A fire mission commences after a JFT entity (P) has detected (P) another entity (P) recognized as a member of the opposing force (C) and is a suitable artillery target (C, E). The JFT (P) must login (P, E) on their Computer (P) through their User Account (V) with appropriate configuration settings such as Privileges (V), Decision Rights (C), Skillsets (C) and Assets (V, P). A Call For Fire message (V) is sent (E) from the JFT to the JFCC. The JFCC entity (P) is able to receive the message (V) after the message has navigated through a network (P) and the underlying network architecture (V). After logging into the system (P, V) the JFCC entity's allocated configuration (V, C) allows it to access the message (V), read the message (P), make a decision (C) and approve the request (V, E). This process includes an assessment of the priority of competing requests for offensive support from different JFT entities. Based on the priority of each specific target to the mission, decisions are made to allocate each fire mission to an Artillery Battery organization (C), which consists of a number of Guns (P, V), managed in a Fire Mission Queue (V). The Call for Fire message (V) and Fire Mission Approval (V) are managed through a series of messages and links on physical devices such as computers (P, V), network devices (P, V) and a network architecture (V, C). The Artillery Battery subsequently performs a series of physical actions to fire the guns and achieve a kinetic effect on a target (P). The fire mission queue (V) is updated to reflect the completion of the assigned fire mission (V). Further interactions between the JFT, JFCC and the Artillery Battery are not modeled but may include battle damage assessment, higher fidelity queue management and voice radio traffic.

In this use case, a compromised node can lead to an effect in the network or other nodes through its capture (P) or through the infection of a machine through a cyber attack (V). Cyber Attacks could target the confidentiality, integrity or availability of any of the actors physical networked assets, their virtual user

accounts, privileges, or messages. Data, both in storage and movement, could also be targeted based on attractiveness and value, such as the grid reference for a target or the location of an actor.
The way that a cyber attack is modeled is through the depiction of each network actor, both physically and virtually, and the different network configurations available. For example, a network configured as a hierarchy with data passing through command nodes will present different challenges to the attacker and defender than a mesh network with a different physical and virtual configuration. Network topologies have been associated with military performance in models and simulation (Dekker 2006). Decision rights have also been considered as part of the command and control architecture (Alberts et al. 2013). User privileges, network configuration settings and the interaction of the various permutations of the network with combat and kinetic effects, when facing a determined and cyber capable adversary, does not appear to have been studied in detail. Organizations will dynamically change in the physical, virtual and conceptual domain as vehicles and personnel are physically damaged or destroyed. Correspondingly, virtual domain changes will result in other domain changes, such as a virus in a node infecting other components of the network leading to denial of service. Layers of inference within the ontology allow an event to cascade through the network.

7 CONCLUSION

In this paper, we have outlined the requirements for several disparate ontologies to answer the question: How do we model and simulate the SoS effects of a cyber attack on an organization or military unit? In doing so, it has produced novel contributions by outlining the domains a potential cyber attack can impact from the perspective of an organization or military unit. We have introduced a comprehensive outline that, once modeled, will provide us with a high level of granularity, allowing a comprehensive simulated response. We have also worked to overcome the limitations inherent in graph modeling across disparate domains through the introduction of an inference layer to the data model. With this layer, we can represent the same sequence of facts at multiple layers without breaking consistency in our data representation. We have also presented a use-case that helps define our requirements, show why we require such disparate ontologies and provides an introduction to our representation and data model.

There are several areas of future work that must be investigated. The most immediate direction is to continue development of each ontology and accurately model the domain of knowledge as it relates to the outlined use-case. After our ontologies have been created and tested independently against multiple use-cases, we then intend to expand our work to ensure their federation is cohesive. From this, we intend to integrate the inference layer and associated software for making these inferences. At this point we intend to begin simulation.

This work has introduced the concept of independent-yet-interoperable ontologies designed to model the multiple domains potentially impacted by a cyber security incident. This work federates these ontologies and has proposed mechanisms for modeling inferred effects independently from their underlying source. Finally, we have created a use-case which will guide our further work and illustrates how our requirements differ from existing systems and concepts.

REFERENCES

Alberts, D. S., F. Bernier, K. Chan, and M. Manso. 2013. *C2 Approaches: Looking for the Sweet Spot.* Alexandria VA: Institute for Defense Analyses

Amin, S. 2011. "On Cyber Security for Networked Control Systems." Masters Thesis, Civil and Environmental Engineering, University of California.

Amoroso, E. 2012. *Cyber attacks: protecting national infrastructure*. New York: Butterworth-Heinemann Elsevier.

Arbuthnot, J. 2013. Defence and Cyber-security: Sixth Report of Session 2012-13, Vol. 1: Report, Together with Formal Minutes, Oral and Written Evidence. TSO Shop.

Argauer, B. 2007. "VTAC: Virtual terrain assisted impact assessment for cyber attacks." Available from: http://scholarworks.rit.edu/theses/3097/ [11 Jun 15], Rochester Institute of Technology.

Barlow, M., and A. Easton. 2002. "Crocadile-an open, extensible agent-based distillation engine." *Information & Security* 8 (1):17-51.

Bernier, M., S. LeBlanc, and B. Morton. 2012. "Metrics Framework of Cyber Operations on Command and Control." Proceedings of the 11th European Conference on Information Warfare and Security. E. Filiol and R. Erra (Eds). Laval, France, Academic publishing international Ltd.

Berzins, V. A. 1999. Re-engineering the Janus (A) combat simulation system. Monterey, California, CA: Naval Postgraduate School.

Bharathy, G. K., L. Yilmaz, and A. Tolk. 2012. "Agent Directed Simulation for Combat Modeling and Distributed Simulation." In *Engineering Principles of Combat Modeling and Distributed Simulation*, edited by A. Tolk, pp669-713. John Wiley & Sons, Inc.

Boyer, B. R. 2011. "Identification and ranking of critical assets within an electrical grid under threat of cyber attack." DOI: http://dx.doi.org/doi:10.7282/T33R0S78, Rutgers, The State University of New Jersey.

Bradshaw, J. M., M. Carvalho, L. Bunch, T. Eskridge, P. J. Feltovich, M. Johnson, and D. Kidwell. 2012. "Sol: An agent-based framework for cyber situation awareness." *KI-Künstliche Intelligenz* 26 (2):pp127-140.

Buchanan, L., M. Larkin, A. D'Amico, L. Buchanan, M. Larkin, and A. D'Amico. 2012. "Mission assurance proof-of-concept: Mapping dependencies among cyber assets, missions, and users." Homeland Security (HST), 2012 IEEE Conference on Technologies for, Waltham, MA, 13-15 Nov. 2012.

Cannon-Bowers, J.A., and E. Salas. 1998. *Making Decisions Under Stress: Implications for Individual and Team Training.* New York, NY: American Psychological Association.

Carr, J. 2010. *Inside cyber warfare: Mapping the cyber underworld*. Sebastopol, CA: O'Reilly Media, Inc.

Cayirci, E., and R. Ghergherehchi. 2011. "Modeling cyber attacks and their effects on decision process." Proceedings of the Winter Simulation Conference.

Charitoudi, K., and A. J. C Blyth. 2014. "An Agent-Based Socio-Technical Approach to Impact Assessment for Cyber Defense." *Information Security Journal: A Global Perspective* 23 (4-6): pp125-136.

Cohen, F. 1999. "Simulating cyber attacks, defences, and consequences." *Computers & Security* 18 (6): pp479-518. DOI: http://dx.doi.org/10.1016/S0167-4048(99)80115-1.

Costa, P., M. Hieb, and A. de Barros Barreto. 2014. "Cyber-Argus: Modeling C2 Impacts of Cyber Attacks." 19th International Command and Control Research and Technology Symposium – C2 Agility: Lessons Learned from Research and Operations, Alexandria, Virginia, USA, June 16-19.

Costantini, K. C. 2007. "Development of a cyber attack simulator for network modeling and cyber security analysis." Available from: https://ritdml.rit.edu/handle/1850/5440 [11 Jun 15], Kate Gleeson College of Technology, Rochester Institute of Technology.

D'Amico, A., L. Buchanan, J. Goodall, and P. Walczak. 2009. "Mission impact of cyber events: scenarios and ontology to express the relationships between cyber assets, missions and users." Proceedings of 5th International Conference on Information Warfare and Security.

Dekker, A. H. 2006. "Agility in networked military systems: A simulation experiment." 11th International Command and Control Research and Technology Symposium, Cambridge, UK.

Epstein, J. M. 1999. "Agent-based computational models and generative social science." *Generative Social Science: Studies in Agent-Based Computational Modeling* 4 (5):4-46.

Fortson Jr, L. W. 2007. Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology. Ohio, USA: Air Force Institute of Technology. Wright-Patterson Air Force Base. School of Engineering and Management.

Frankel, M.S. 2000. *Report of the Defense Science Board Task Force on Tactical Battlefield Communications*, Available from:

http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA373829. Washington, DC, USA.: Defense Science Board, Department of Defense.

Goodall, J R., A. D'Amico, and J. K. Kopylec. 2009. "Camus: Automatically mapping cyber assets to missions and users." Military Communications Conference, 2009. MILCOM 2009., Boston, Massachusetts, USA.

Grimaila, M. R., and A. Badiru. 2011. "A hybrid dynamic decision making methodology for defensive information technology contingency measure selection in the presence of cyber threats." *Operational Research* 13 (1):67-88.

Grimaila, M. R., L. W. Fortson, and J. L. Sutton. 2009. Design considerations for a cyber incident mission impact assessment (CIMIA) process. DTIC Document.

Gruber, T. R. 1993. "Toward principles for the design of ontologies used for knowledge sharing?" In *Formal Ontology in Conceptual Analysis and Knowledge Representation*, edited by N. Guarino and R. Pol, p1. Palo Alto, CA: Kluwer Academic Publishers.

Holsopple, J., and S. J. Yang. 2008. "FuSIA: future situation and impact awareness." Information Fusion, 2008 11th International Conference on.

Holsopple, J., S. J. Yang, and M. Sudit. 2015. "Mission Impact Assessment for Cyber Warfare." In *Intelligent Methods for Cyber Warfare*, 239-266. Springer.

Ilachinski, A. 2004. *Artificial war: Multiagent-based simulation of combat.* Singapore.: World Scientific.

Jackson, M. C., and P. Keys. 1984. "Towards a System of Systems Methodologies." *The Journal of the Operational Research Society* 35 (6):473-486. doi: 10.2307/2581795.

Konstantinia, C., and B. Andrew. 2013. "A Socio Technical Approach to Cyber Risk Management and Impact Assessment." *Journal of Information Security* 4:33-41.

Kotenko, I. 2010. "Agent-based modelling and simulation of network cyber-attacks and cooperative defence mechanisms." *Discrete Event Simulations. Sciyo, In-teh*:223-246.

Kott, A., C. Wang, and R. Erbacher. 2014. *Cyber Defense and Situational Awareness*, Available from: http://site.ebrary.com/lib/unsw/docDetail.action?docID=11005825 [11 Jun 15]. Cham, DEU: Springer International Publishing.

Kundur, D., X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry. 2011. "Towards modelling the impact of cyber attacks on a smart grid." *International Journal of Security and Networks* 6 (1):pp2-13.

Lauren, M., and R. Stephen. 2002. "Map-aware non-uniform automata (MANA)-a new zealand approach to scenario modelling." *Journal of Battlefield Technology* 5:27-31.

Leed, M. 2013. "Offensive Cyber Capabilities at the Operational Level." *Center for Strategic International Studies*.

Liff, A. P. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35 (3):pp401-428.

Llanso, T., and E. Klatt. 2014. "CyMRisk: An approach for computing mission risk due to cyber attacks." Systems Conference (SysCon), 2014 8th Annual IEEE.

Lucas, T. W., and S. M. Sanchez. 2003. Smart experimental designs provide military decision-makers with new insights from agent-based simulations. Monterey, CA.: Naval Postgraduate School Operations Research Department.

Maughan, D. 2009. A roadmap for cybersecurity research. edited by INFOSEC Research Council (IRC). Washington, DC. USA.: US Department of Homeland Security.

Musman, S., and S. Agbolosu-Amison. 2014. A Measurable Definition of Resiliency Using "Mission Risk" as a Metric. McLean, VA: Mitre Corp.

Musman, S., M. Tanner, A. Temin, E. Elsaesser, and L. Loren. 2011. "Computing the impact of cyber attacks on complex missions." Systems Conference (SysCon), 2011 IEEE International.

Negrete-Pincetic, M., F. Yoshida, and G. Gross. 2009. "Towards quantifying the impacts of cyber attacks in the competitive electricity market environment." PowerTech, 2009, Bucharest, 28 June - 2 July.

Nesteruk, E. A. 2009. "Security considerations for network-centric weapon systems." Available from: http://calhoun.nps.edu/handle/10945/4584 [11 Jun 15], Naval Postgraduate School.

Ratcliff, R. A. 2006. *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers*. London, UK: Cambridge University Press.

Robinson, N., L. Gribbon, V. Horvath, and K. Robertson. 2013. Cyber-security threat characterisation. In *Prepared for the Swedish National Defence College, Stockholm*. Santa Monica, CA: RAND Corporation.

Robinson, S. 2008. "Conceptual modelling for simulation Part I: definition and requirements." *Journal of the operational research society* 59 (3):278-290.

Robinson, S. B. 2009. "A modeling process to understand complex system architectures." Available from: https://smartech.gatech.edu/handle/1853/29621 [11 Jun 15], School of Aerospace Engineering, Georgia Institute of Technology.

Sage, A. P., and C. D. Cuppan. 2001. "On the systems engineering and management of systems of systems and federations of systems." *Information, Knowledge, Systems Management* 2 (4):325-345.

Schramm, H. C., and D. P. Gaver. 2013. "Lanchester for cyber: The mixed epidemic-combat model." *Naval Research Logistics (NRL)* 60 (7):599-605.

Straver, M. C., E. Vincent, and P. Fournier. 2006. "Experiences with the MANA simulation tool." *Defence Research and Development Canada (DRDC) Valcartier Operational Research Team. Technical Memorandum DRDC Valcartier TM* 404.

Tolk, A. 2012. "Modeling Communications, Command, and Control." In *Engineering Principles of Combat Modeling and Distributed Simulation*, edited by A. Tolk, pp171-183. Hoboken, New Jersey: John Wiley & Sons, Inc.

Tolk, A., N. R. Adam, E. Cayirci, S. Pickl, R. Shumaker, J. A. Sullivan, and W. F. Waite. 2012. "Defense and security applications of modeling and simulation—Grand challenges and current efforts." Simulation Conference (WSC), Proceedings of the 2012 Winter.

US Department of Defense. 2013a. Joint Publication 3-12 (R) - Cyberspace Operations. Washington, DC. USA.

US Department of Defense. 2013b. Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. edited by Defense Science Board. Washington, USA: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

US Department of the Army. 2012. ADRP 3-0 Unified Land Operations. edited by Department of Defense. Washington, USA.

Van Creveld, M. 1985. *Command in war*. New York, NY.: Harvard University Press.

Vieira, A. C., S. H. Houmb, and D. R. Insua. 2014. "A Graphical Adversarial Risk Analysis Model for Oil and Gas Drilling Cybersecurity." The International Workshop on Graphical Models for Security 2014.

Watters, J., S. Morrissey, D. Bodeau, and S. C. Powers. 2009. "The risk-to-mission assessment process (RiskMAP): a sensitivity analysis and an extension to treat confidentiality issues." *The Institute for Information Infrastructure Protection*.

Weber, E. P., and A. M. Khademian. 2008. "Wicked problems, knowledge challenges, and collaborative capacity builders in network settings." *Public administration review* 68 (2):334-349.

Wittman Jr, R. L., and J. Surdu. 2005. "OneSAF objective system: toolkit supporting user and developer lifecycles within a multi-domain modeling and simulation environment." Simulation conference and exhibition (SimTecT 2005), Sydney, Australia.

AUTHOR BIOGRAPHIES

DAVID ORMROD is an Australian Army officer and Ph.D. Candidate studying at the Australian Defense Force Academy in Canberra, ACT. He is the Chief of Army Foundation Scholar for 2015. His thesis topic is 'Managing the risks of information deception upon tactical C4ISR systems used for land combat'. David has served on operations in Iraq and worked with the British Army in Germany. He holds a Masters of Information System Management, Masters of Management Studies, Graduate Diploma in Adult Education and a Bachelors Degree. He is a member of INFORMS, AISA, ACM, IEEE and is a Project Management Professional with the PMI. His e-mail address is david.ormrod@defence.gov.au.

BENJAMIN TURNBULL is a Lecturer at the University of New South Wales Canberra at the Australian Defense Force Academy in Canberra, ACT. He holds a Ph.D. in Digital Forensics and a Bachelor in Information Technology from the University of South Australia, and has previously worked as a Research Scientist for the Defense Science and Technology Organization and as a National Drug Law Enforcement Research Fund Post-Doctorate Research Fellow. His research interests include Cyber Situational Awareness and Cyber Decision Support. His email address is b.turnbull@adfa.edu.au.

KENT O'SULLIVAN is an Australian Army officer and is currently a Chief of Army's honors student undertaking study in Cyber Security at the Australian Defense Force Academy in Canberra, ACT. He holds a Bachelor of Information Technology from the University of New South Wales and is currently undertaking research into the design of cyber defense ontologies for use in military simulation. His email address is kent.osullivan@defence.gov.au.