2015

The cyber simulation terrain: Towards an open source cyber effects simulation ontology

Kent O'Sullivan
Australian Centre for Cyber Security, University of New South Wales, kent.osullivan@defence.gov.au

Benjamin Turnbull
Australian Centre for Cyber Security, University of New South Wales, b.turnbull@adfa.edu.au

DOI: 10.4225/75/57a84e3bbefbc
Originally published in the Proceedings of the 16th Australian Information Warfare Conference (pp. 14-23), held on the 30 November - 2 December, 2015, Edith Cowan University, Joondalup Campus, Perth, Western Australia.

THE CYBER SIMULATION TERRAIN: TOWARDS AN OPEN SOURCE CYBER EFFECTS SIMULATION ONTOLOGY

LT Kent O'Sullivan, Dr Benjamin Turnbull
Australian Centre for Cyber Security, University of New South Wales, Canberra, Australia
kent.osullivan@defence.gov.au, b.turnbull@adfa.edu.au

Abstract

Cyber resilience is characterised by an ability to understand and adapt to changing network conditions, including cyber attacks. Cyber resilience may be characterised by an effects-based approach to missions or processes. One of the fundamental preconditions underpinning cyber resilience is an accurate representation of current network and machine states and what missions they are supporting. This research outlines the need for an ontological network representation, drawing on existing literature and implementations in the domain. This work then introduces an open-source ontological representation for modelling cyber assets for the purposes of Computer Network Defence. This representation encompasses computers, network connectivity, users, software, vulnerabilities and exploits and aims for interoperability with related representations in common use. The utility of this work is highlighted against a functional use-case depicting a realistic operational network and mission. Finally, a future research direction is defined.

Keywords
Cyber, Simulation, Cyber Effects, Ontology, Cyber Terrain, Virtual Terrain, CESO, CST, Cyber Simulation Terrain, Cyber Effects Simulation Ontology, Land Power, Futures, Cyber-Dependence Paradox, Cyber Resilience

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.

INTRODUCTION

On the modern battlefield, the integrity of the cyber systems supporting operations is paramount. A commander who requires precision fires to support mission objectives relies heavily on their networked Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities to deliver these effects. Compromise of these systems by an opposing force will deny a commander unimpeded use of their capabilities and lead to probable mission failure. Understanding the interrelation of these systems with the physical and human systems of the battlespace is essential to developing an understanding of their potential vulnerabilities and developing resilience strategies. The effect of a cyber attack is nuanced, and its impact on assets and capabilities is often not immediately apparent against mission objectives. We seek to address these challenges with this work.

BACKGROUND

The Australian Army's Future Land Warfare Report (MSP-A, 2014b) describes a future where militaries will require that future conflict is "waged by information technology enabled forces in land, sea, air, space and cyberspace" (MSP-A, 2014a, p8). Militaries will "use modern information technology to link sensors, weapons systems, commanders and their personnel in a networked environment" (MSP-A, 2012, p60). Globally, militaries are developing cyber doctrine (JSDO, 2013) scoping the offensive use of cyber capabilities -the United States Army has even integrated proformas for Computer Network Attack and Cyber Effect requests, and Cyberspace Operations Mission Task orders into doctrine (USA, 2013).

The new digital networked battlespace presents a paradox. To operate effectively in this future environment, military forces are exploiting C4ISR networks to provide unprecedented levels of command and control (Ormrod 2014a). A military force's reliance on these systems to operate effectively can quickly become dependence and bring vulnerability (Ormrod, 2014b). The British identify networked C2 as a key enabler of their ability to effectively conduct manoeuvre warfare (DJFCD, 2012). The US Army also recognises this paradox (DJFCD, 2012, p.v) and identify that their superior networked C2 capabilities are a likely target for enemy forces seeking to disrupt their command and control and neutralise their technological advantage (USATDC, 2014).

The significance of this exposure creates an imperative to investigate means to prevent cyber attacks from occurring and plan for disaster recovery, preparing for the probability of operating in an information degraded environment (Scott, 2013). Understanding these problems and preparing for their eventuality is working towards creating organisational cyber resilience. Cyber resilience is premised on:

> The current philosophy of trying to keep the adversaries out, or the assumption that they will be detected if they get through the first line of defense, is no longer valid. Given the sophistication, adaptiveness, and persistence of cyber threats, we can no longer assume that we can completely defend against intruders and must change our mindset to assume some degree of adversary success and be prepared to "fight through" cyber attacks to ensure mission success even in a degraded or contested environment (Goldman, McQuaid, Piccotto, 2011, p1).

The United States Air Force extends this approach and actively advocates for the need to contextualise the impact of cyber attack from a mission perspective, stating:

> The time has come to think of cyberspace in a new light; not only must we defend against any attack, we must be able to "fight through" any attack, accomplish our missions and retain the ability to respond–thus giving us mission assurance in the face of future attacks or other disruptions (USAFSC, 2009, p4).

One of the first prerequisites of a "fight through [approach to cyber resilience is] ...to map USAF network to USAF missions with end-to-end forensics approach*"* (USAFC, 2009, p11). Work related to these documents, if any, is not in the public domain. Consequently, there is little research that adequately models the cyber domain from a mission assurance and security impact perspective.

Planning For A Resilient Future

There are a near-infinite number of possible scenarios for which a resilient organisation must prepare. A futures view of developing resilience requires decision makers to consider the possibilities, enumerate the plausibilities and deduce the probable issues that they will encounter, enabling the decision maker to determine what actions need to be taken to guide their organisation towards a preferable future state (Hajkowicz, 2015). Anticipating problems and developing contingencies increases resilience.

Computer networks and cyberattacks interact with the battlefield and decision makers as a collection of inextricably linked systems of systems. The complexity of the systems, issues of system to decision maker trust, the inherent uncertainty of complex interactions and the resulting emergent phenomena intersect to form a wicked problem for decision makers (Ormrod, 2014b), making the enumeration of futures extremely challenging.

To understand the complexities of these systems, we must clearly identify the entities, properties and relationships of the systems. To achieve this, we apply a network approach. Philosophically, networks are simply a collection of concepts with defined interrelations. Complex systems are are collections of entities that interact - fitting the network model. The benefit of applying a defined network structure to deconstruct complexity is that it formalises the representation and enables analysts to validate the Emergent Phenomena of the network. Emergent Phenomena are collective behaviours observed in network interactions. These phenomena offer the best window of insight into possible futures. The generation of phenomena is highly dependent on the underlying network structure (Caldarelli, Catanazro 2012). We have elected to use ontological structures to reliably represent the complex systems of cyber-physical-cognitive interaction on the battlefield as networks.

An ontology is an explicit specification of a shared conceptualization (Gruber, 1995). It is a unifying framework that unites multiple viewpoints facilitate problem solving (Uschold, Gruninger, 1996). A 'strong' ontology is judged by its real-world semantics, use of logical axioms and machine readability (Obrst, 2010). They are built by collecting and integrating numerous subject-predicate-object triples. Each triple should define a single fact within the ontology. The effectiveness of this triple to represent only a single fact reflects the triple's semantic strength. In the context of the big data problems associated with modelling complex systems of systems a semantically strong ontology will optimise searching, promote automation and efficiency of scale.

The Cyber Simulation Terrain (CST) proposed in this paper is the explicit definition of the concepts, properties and relationships of the complex system that is organisational cyber-infrastructure. It is a component of the Cyber Effects Simulation Ontology (CSEO) - an effort to model the effects that cyber attacks have on a computer system as part of a larger, more complex interconnection of systems. The transparent semantic strength of the CESO and CST will permit validation of observed emergent phenomena, enhancing the credibility of simulations modelling the interactions of cyber effects on land forces in combat enabling future organisational shaping towards resilience.

RELATED WORK

Representation of computer networks to facilitate analysis of vulnerabilities, attack vectors and mission-node criticality has a long history. Initially work was focused on graphing approaches to the problem (Phillips, Swiler 1998; Swiler, Phillips, Ellis 2001; Sheyner, et. al, 2002), utilising probabilistic statistical models to deduce current and future states and attack paths. Limitations of scalability and fidelity contributed to supersession by information fusion approaches. These approaches seek to efficiently exploit data collected by intrusion detection sensors to generate probabilistic models of likely attack vectors and future network states. The INFERD (Sudit et. al, 2006) and ECCARS (Sudit, Stotz, Holender, 2005) models were among the first major steps to achieving an effective information fusion solution.

TANDI evolved from similar ideas, choosing to isolate the logical network topology from the predictive model (Holsopple, Yang, Sudit, 2006). Independent topology or 'terrain' models are a core feature of many of the subsequent information fusion approaches. VTAC (Argauer 2008), FuSIA (Holsopple, Yang, 2008), CAMUS (Goodall, D'Amico, Kopylec, 2009) and the High-Level Information Fusion for Tracking and Projection of Multistage Cyber Attacks (Yang et. al, 2009) all utilised independent terrain models.

Independent terrain models are also used in mission impact analysis as part of the CSIM (Jakobson, 2011a; Jakobson 2011b; Jakobson 2013). They have been influential on the development of the Cyber-ARGUS framework that models the command and control impacts of cyber attacks (Barreto 2012; Barreto 2014) and the modelling of cyber situational awareness (Machado, Barreto, Yano, 2013; Machado, Yano 2014). It has demonstrated utility in supporting cyber attack simulation, present in the CyberSim Modular Cyber Attack Simulator (Moskal et. al, 2013), MASS (Moskal et. al, 2014) and CASCADES (Wheeler, 2014; Kreider, 2015).

All of these approaches have evolved out of the independent Cyber-Virtual Terrain model that was put forward by Fava et. al (2007). Their paper applied an independent terrain model to complex multistage cyber attacks. The catalyst for the development of independent terrain models, however, is the Virtual Terrain (VT) model (Holsopple et. al, 2008). The VT model encapsulates the Cyber Virtual Terrain and defines the core elements of terrain models that endure across its evolutions.

The VT core evolved in the Virtual Terrain version 2 (VT.2) to include the capacity to represent incomplete network information, include a more accurate depiction of internet connectivity and represent routers exclusively as traversal nodes. (Moskal et. al, 2013; Moskal et. al, 2014). The most recent iteration of the VT is the Dynamic Virtual Terrain (DVT) (Wheeler, 2014). Like VT.2, the DVT is intended to support cyber-attack simulations. The DVT is a significant revision of the VT and VT.2. Its key aim is to facilitate the simulation of Moving Target Network Defence Measures (MTNDM) such as IP address hopping and port hopping. The Cyber Terrain (CT) developed by Jakobson in 2011 (Jakobson 2011a; 2011b) has evolved from the original VT to support mission planning and resilience building.

Each of these terrains was assessed for their suitability for inclusion into the CESO. However, lack of publicly available schema has prevented a detailed suitability analysis. Based on the publicly available information, a consistent issue is a lack of granularity. CVT, VT, VT.2 and DVT simplify representation at the cost of fidelity. The mapping of nodal interdependencies by the VT family of models is not sufficient to realistically represent the network. CT maps the dependencies in a granular manner but then abstracts much of the nodal detail that makes the VT family of models useful. DVT has stepped further away from reality, centralising many functions of the network - modifying and abstracting the terrain structure to represent MTNDMs. Existing terrain models also do not address the actual flow of information across the network, sessional communication between nodes, wireless as its own use-case, data spill or virtualisation.

The CST adopts the CT approach to dependency mapping with the philosophy of the VT family of terrains - gearing towards the simulation of cyber attacks. It will do this at greater levels of granularity and maximise interoperability with linked efforts such as the MITRE standards and the Structured Threat Information eXpression (STIX) (Barnum, 2012). The semantic strength of this ontological structure will enable validation of results generated by simulations and analysis, maximising the efficacy of the predicted future states it represents.

THE CYBER SIMULATION TERRAIN

The purpose of the CST is to accurately model the assets and systems across a computer network. The representation must be generic enough to encompass corporate networks also extensible enough to model bespoke and operational systems. Modelling a computer network has several benefits; a comparison between network sensors and predefined models allow for rogue and masquerading device detection, an understanding of impact from hypothetical scenarios across realistic infrastructure, allows for a greater and immediate understanding of the impact of a cyber-security incident, and to understand the impact of a cyber-security

incident on business processes or missions. Finally, a detailed computer and network model can be used for research-based simulation.

Although government publicly advocates endpoint protection (Australian Signals Directorate, 2012) and there are multiple commercial implementations (FireEye; CYLANCE; Bromium; SentinelOne; Bit9; EMC 2015), most of the benefits of these tools relate to blocking infection, reporting endpoint state and patch status, and remote forensic acquisition. There is little work on modelling the network state and shape over time against known states. Changes to the expected behaviour of objects or network shape, caused by misconfiguration, device masquerading or rogue devices, can be easily detected through comparisons to models representing the predefined 'normal' network.

A comprehensive cyber security model can also be used to test hypotheses against a network for impact analysis. An example of this was the announcement of the OpenSSL Heartbleed vulnerability (Codenomicon, 2015). Immediately after its publication and public disclosure, there was little understanding of the impact of the exploitable vulnerability across the network. In some cases, it took several days for providers to fully appreciate the effects to internal systems, operations and data. A network model allows for new vulnerabilities and exploits to be tested against a particular network system to determine immediate impacts and ongoing leverage points. These can be injected into the model and their impact tested without endangering an operational environment. The CST is designed to accomplish these aims.

The CST Schema is open source and available at:

https://github.com/AustralianCentreforCyberSecurity/Cyber-Simulation-Terrain

Public availability makes the ontology unique in that it is available for critique and analysis. The repository also contains several use-cases that highlight its intended use. The schema has been implemented using the Resource Description Framework (RDF) (RDF Working Group, 2014a) Turtle (TTL) (RDF Working Group 2014b) syntax with minimal elements of the Ontology Web Language (OWL) (OWL Working Group, 2012). Queries are performed using the Sparql Protocol And Rdf Query Language (SPARQL) (SPARQL Working Group, 2015). The CST Schema has been designed to achieve granularity in content and structure in representation. Figure 1 depicts the schema. The blue nodes represent the concepts or objects in the ontology. The red represent properties (will be leaf nodes) and relationships (will be traversal nodes). The visualisations in this paper were created using the easyRDF converter (Humfrey, 2015) and the RDFGravity Visualisation Tool (Goyal, Westenhaler, 2015).

Schema

The CST is an interconnection of nodes. Nodes can be specialised as computers, routers, IDS sensors or Domain Controllers. Nodes connect to Subnetworks through a Network Interface Controller (NIC) (including wireless and virtual nodes). Computer MAC and IP addresses are associated with their NIC, permitting the representation of a computer belonging to multiple physical, virtual and wireless networks via multiple interfaces. Subnetworks connect to each other and the internet through a router. A router will have defined routes that control the traffic flow across the network between subnets. The internetwork is the network of routers - a conceptual addition that assists in modelling the interconnection of subnets.

Computers will have associated software and services. These concepts are arranged hierarchically in a similar manner to the Virtual Terrain *service tree* concept. Computers are associated with an installed version of software. That installed version will be associated with a parent software type class to facilitate categorisation and querying. The more granular relationships are to the service that software projects when running on the computer and any known vulnerabilities associated with a piece of software. Zero-days are represented as an exploit related to a vulnerability, but will have no links to a CVE or other published vulnerability. Software versions are associated with their CPE ID (MITRE, 2015a), vulnerabilities with their CVE identifier (Martin, 2001) and weakness types are associated with a CWE (MITRE 2015b) number. Metrics of criticality and exploitability associated with vulnerabilities utilise the CVSS (FIRST CVSS SIG, 2015) scores. The intention of integration with these standards is to leverage the existing resources, maximise the interoperability of the CST with the wider CESO as one of the modules. The vulnerability association is also the interface with the 'red team' elements of the CESO, an abridged implementation of STIX, also aims to leverage existing work and maximising interoperability.

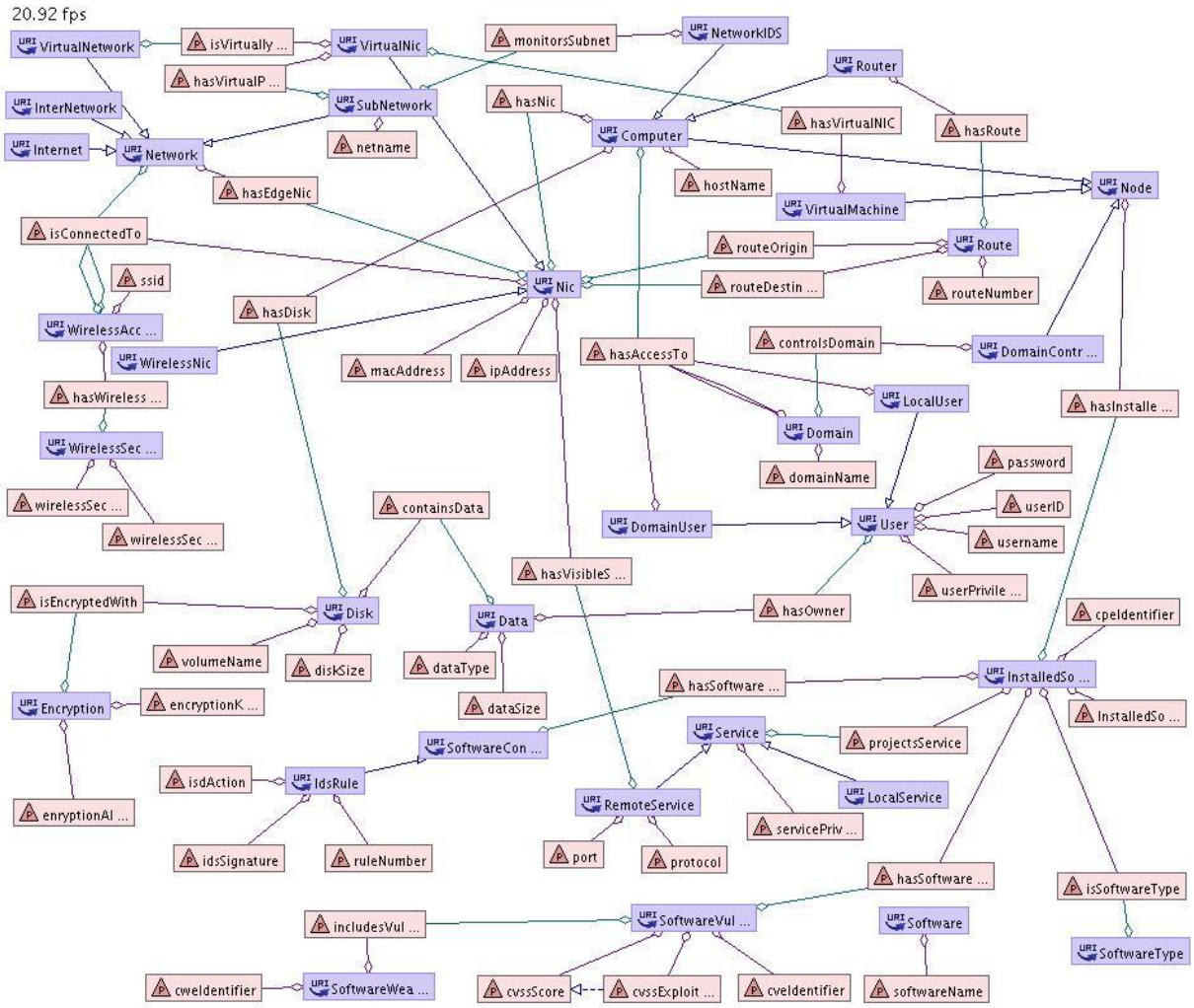

Figure 1 - CST Schema

Installed software runs either local or remote services. Local services run internally to the node, and remote services project their Service Name, Port Number and Protocol to the NIC connected to their computer forming an implicit host-based firewall - if a service has a port open on the network card, it is assumed to be listening. If it is not listening it will not be shown. Services also have an associated privilege level. These privilege levels map to the privilege levels associated with users. If a user has a privilege level that matches the service, they can interact with it. Users can be associated with a computer either locally or as part of a domain. Local users can access only a computer with which they have an explicit link. Domain users belong to a domain that can have multiple member computers. Domain users can access any computer in a domain to which they are authenticated. Domains have a domain controller that connects to a single subnet but can control domains across multiple subnets. There can be multiple domains per subnet and multiple domains per computer, allowing us to represent a user who might have a secret and an unclassified domain account on the same computer and accounting for data-spill use-cases. Users are owners of their data. Data is stored locally on computers on a disk. The disks can be encrypted or unencrypted. If encrypted, a user has to authenticate to access the data.

Intrusion detection and antivirus is implemented at the host level. A host-based signature IDS is represented as a running service on a node. The IDS links to a signature database that will consist of the unique identifiers matching vulnerabilities and exploits. The IDS has configurable rules that are a subtype of the software configuration concept linked to the installed version of the software. These rules allow the IDS to be 'tuned' by selecting the signature and action on detection. MTNDMs can be represented in the CST by its linkage to the CESO Event Ontology.

EXAMPLE USE CASE

The use-case implemented below is drawn from the paper defining the CESO (Ormrod, Turnbull, O'Sullivan, In-Press). It depicts the process required for a Joint Fires Team (JFT) to call for Offensive Support (OS), the call for fire to be handled by a Joint Fires Communication Centre (JFCC) and have the mission fired by an Artillery Battery. Figure 2 visualises the required cyber infrastructure to conduct this task. It does not demonstrate the full capabilities of the terrain but is a proof-of-concept of the most commonly used features.

The use-case depicts three subnetworks connected by routes on the same router - the JFT Network, the JFCC Network and the Artillery Battery Network. All computers on these networks are members of the 'Joint Fires' Domain and are accessible by all authenticated users. Computers are running a mix of local and remote software and services (services are fabricated for this use-case). The JFT has Targeting and Request for Fires Communications software. They use this to communicate with the JFCC, who use their Mission Control software to push the fire mission to the Artillery Battery HQ. The communications between the JFCC and the Artillery Battery HQ are encrypted. However, the software that they are using is an older version of OpenSSL that is still vulnerable to Heartbleed. The Battery HQ uses their Battery Management Software to push the fire missions to individual Artillery Troops who use their Fire Control Software to prosecute the fire mission.

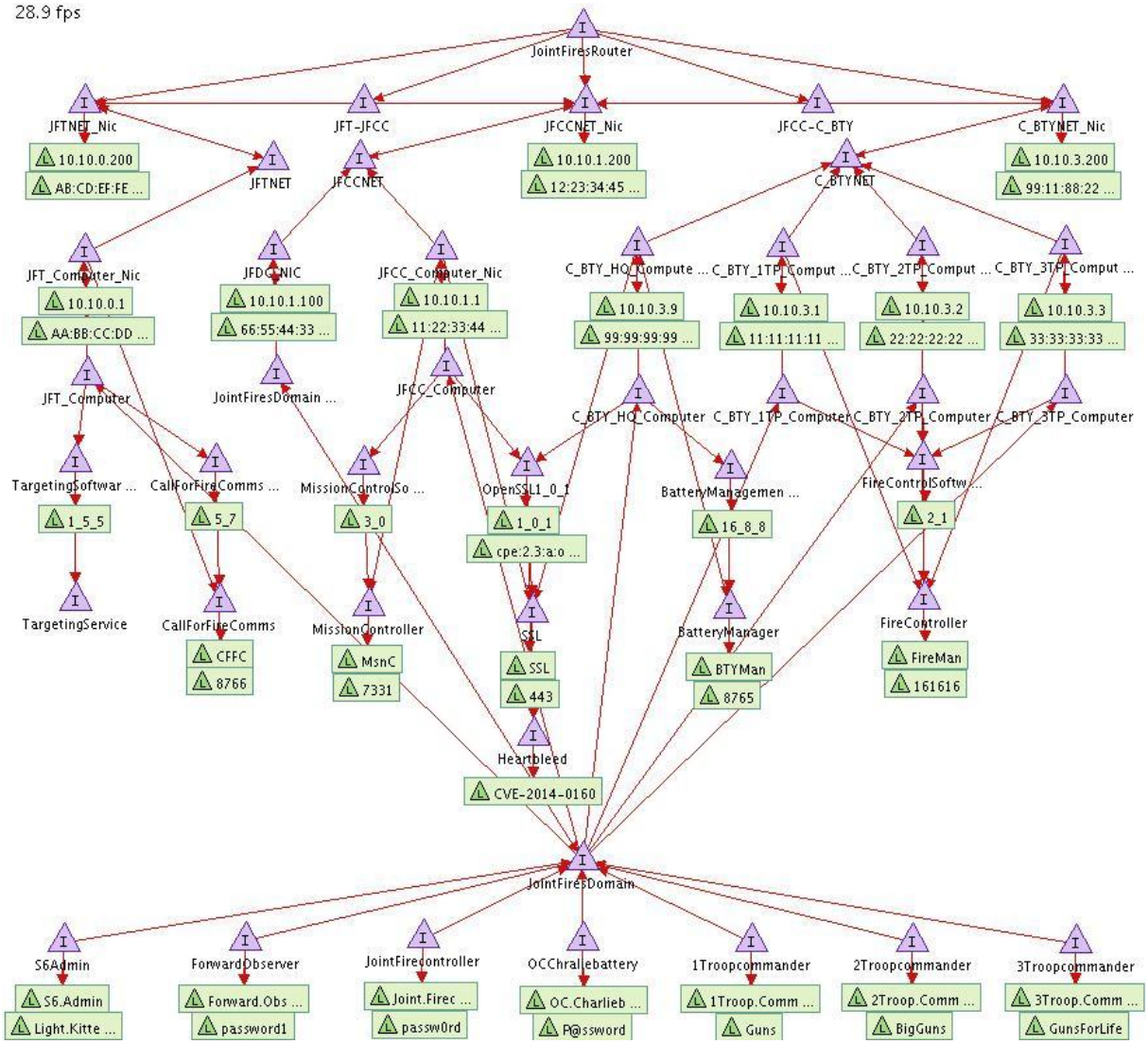

Figure 2 - CST Call for Fire use-case visualisation

In addition to effectively representing this use-case, the CST can also elicit information about the network. Figure 3 shows the results of queries run against the use-case. The first query can quickly produce information about computer and network attributes. The second query checks for the presence of known vulnerabilities,

detecting Heartbleed on the JFCC and Battery HQ computers. Query three then returns all known information about the vulnerability.

These are only a small subset of the queries that the CST uses to determine possible, plausible and probable futures. The emergent phenomena(potential future state) in this use-case is the potential relationship that an actor attacking the network has with the Heartbleed vulnerability. The attacker could compromise the confidentiality of that link, use it to intercept communications and learn of the impending fire mission, and warn the targets of the fire mission, potentially giving the enemy time to evade or prepare counter-battery fire in response to the attack. These fascinating and relevant second and third order effects are not knowable from looking at information in isolation. A decision maker who learns that a probable future has their OS capability rendered ineffective by an enemy at a time of their choosing will likely wish to take actions (such as patching the vulnerability) to move towards a preferable future where their OS capability remains effective.

Figure 3 - CST Use-case - SPARQL Query Results

CONCLUSION AND FUTURE WORK

In this paper we have outlined the requirement and initial implementation of a publicly-available ontological schema designed to assist in Cyber Security Research. There are several areas of future work arising from this; the highest priority of these being the continual improvement and refinement of the ontological schema. Beyond this, it is expected that the ontology will evolve over time as new concepts arise, new network designs emerge, and additional information is required. Some of these changes will be minor, and some may require backwards-incompatible changes. As these occur testing, harnesses and deployments will be updated.

The biggest area of future work is in the development of systems to populate, reason on and visualise this ontology. There are also multiple defined use-cases that require further development. There are precedents for the automated detection and ingestion of data sources and several associated challenges (Moir, Dean, 2015; Grove et. al, 2013) that will guide these efforts. The first stage of development will be to support automated simulation development and analysis.

REFERENCES

Argauer, B. J, & Yang, S. J. (2008). VTAC: Virtual terrain assisted impact assessment for cyber attacks. Paper presented at the SPIE Defense and Security Symposium.

Australian Signals Directorate (2012). Top four mitigation strategies to protect your ICT system. Canberra, ACT: Department of Defence Retrieved from http://www.asd.gov.au/publications/protect/Top_4_Mitigations.pdf.

Barnum, S. (2012). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). MITRE Corporation.

Barros Barreto, A, Costa, P, & Hieb, M. (2014). Cyber-Argus: Modelling C2 impacts of Cyber Attacks. Paper presented at the 19th International Command And Control Research and Technology Symposium, Alexandria, Virginia, USA.

Barros Barreto, A, Costa, P. C, & Yano, E. T. (2012). A Semantic Approach to Evaluate the Impact of Cyber Actions on the Physical Domain. Paper presented at the The Seventh International Conference on Semantic Technology for Intelligence Defence and Security, George mason University, Fairfax, Virginia.
Bit9. (2015). Bit9 and Carbon Black Endpoint Protection Solution. Retrieved October 18, 2015, from https://www.bit9.com/solutions/bit9-carbon-black-solution/

Bromium. (2015). Endpoint Security Products Overview. Retrieved 18 October, 2015, from http://www.bromium.com/products.html
Caldarelli, G, & Catanzaro, M. (2012). Networks: A Very Short Introduction. Oxford, UK: Oxford University Press.

Codenomicon. (2015). The Heartbleed Bug. Retrieved 22 Jun 2015, 2015, from http://heartbleed.com/

CYLANCE. (2015). CYLANCE Protect. Retrieved 18 October, 2015, from http://www.cylance.com/products/protect/
Director Joint Forces (Concepts and Doctrine). (2012). Joint Concept Note 02/12: The Future Land Operating Concept. (JNC02/12). Shirvenham, Swindon, Wiltshire: The Development, Concepts and Doctrine Centre.

EMC Corporation. (2015). EMC RSA ECAT. Retrieved 18 October, 2015, from http://australia.emc.com/security/rsa-ecat.htm
Fava, D, Holsopple, J, Yang, S. J, & Argauer, B. (2007). Terrain and behavior modeling for projecting multistage cyber attacks. Paper presented at the 2007 10th International Conference on Information Fusion.

FireEye. (2015). Endpoint Security. Retrieved 18 October, 2015, from https://www.fireeye.com/products/hx-endpoint-security-products.html
Forum of Incident Response and Security Teams CVSS Special Interest Group (2015). Common Vulnerability Scoring System Version 3.0 Specification Document. Retrieved 18 October, 2015, from https://www.first.org/cvss/cvss-v30-specification-v1.7.pdf

Goldman, H, McQuaid, R, & Picciotto, J. (2011). Cyber resilience for mission assurance. Paper presented at the 2011 IEEE International Conference on Technologies for Homeland Security (HST).
Goodall, J. R, D'Amico, A, & Kopylec, J. K. (2009). Camus: Automatically mapping cyber assets to missions and users. Paper presented at the 2009 IEEE Military Communications Conference (MILCOM).

Goyal, S, & Westenthaler, R. (2015). RDF Gravity (RDF graph visualization tool). Retrieved 14 October, 2015, from http://semweb.salzburgresearch.at/apps/rdf-gravity/
Grove, D, Murray, A, Gerhardy, D, Turnbull, B, Tobin, T, & Moir, C. (2013). An overview of the parallax BattleMind v1. 5 for computer network defence. Paper presented at the Proceedings of the Eleventh Australasian Information Security Conference-Volume 138.

Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing. International journal of human-computer studies, 43(5), 907-928.
Hajkowicz, S. (2015). Global megatrends: Seven Patterns of Change Shaping Our Future (1 ed.). Clayton South, VIC: CSIRO Publishing.

Holsopple, J, Yang, S, & Argauer, B. (2008). Virtual terrain: a security-based representation of a computer network. Paper presented at the 2008 SPIE Defense and Security Symposium.

Holsopple, J, & Yang, S. J. (2008). FuSIA: Future situation and impact awareness. Paper presented at the 11th International Conference on Information Fusion.

Holsopple, J, Yang, S. J, & Sudit, M. (2006). TANDI: Threat assessment of network data and information. Paper presented at the Defense and Security Symposium.

Humfrey, N. (2015). easyRDF Converter. Retrieved 18 October, 2015, from http://www.easyrdf.org/converter

Jakobson, G. (2011a). Extending situation modeling with inference of plausible future cyber situations. Paper presented at the 2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA).

Jakobson, G. (2011b). Mission cyber security situation assessment using impact dependency graphs. Paper presented at the 2011 14th International Conference on Information Fusion.

Jakobson, G. (2013). Mission-centricity in cyber security: Architecting cyber attack resilient missions. Paper presented at the 5th International Conference on Cyber Conflict (CyCon), Talinn, Estonia. https://ccdcoe.org/cycon/2013/proceedings/d1r2s1_jakobson.pdf

Joint Staff Director of Operations. (2013). Joint Publicaton 3-12: Cyberspace Operations. Suffolk, VA.

Kreider, D. (2015). A Guidance Template for Attack Sequence Specification in Cyber Attack Simulation. (Master of Science (Industrial Engineering) Masters), Rochester Institute of Technology, Rochester. Retrieved from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=9941&context=theses

Machado, A. F, Barreto, A. B, & Yano, E. T. (2013). Architecture for cyber defense simulator in military applications. Paper presented at the 18th Annual Command & Control Research & Technology Symposium (ICCRTS), Alexandria, Virginia, USA.

Machado, A. F, & Yano, E. T. (2014). Conceptual Architecture for Obtaining Cyber Situational Awareness. Paper presented at the 2014 18th International Command & Control Research & Technology Symposium (ICCRTS), Alexandria, VA.

Martin, R. (2001). Managing vulnerabilities in networked systems. IEEE Computer Society Computer Magazine, 34, 32-38.

MITRE Corporation. (2015a). The Common Platform Enumeration Specification. Retrieved 18 October, 2015, from https://cpe.mitre.org/specification/

MITRE Corporation. (2015b). The Common Weakness Enumeration, Retrieved 18 October, 2015, from https://cwe.mitre.org/

Modernisation and Strategic Planning Division – Australian Army Headquarters (2012). Adaptive Campaigning: Future Land Operating Concept. (ACFLOC). Canberra, ACT: Australian Army.

Modernisation and Strategic Planning Division – Australian Army Headquarters. (2014a). The Fundamentals of Land Power. (LWD-1). Canberra, ACT: Australian Army.

Modernisation and Strategic Planning Division – Australian Army Headquarters (2014b). The Future land Warfare Report. (FLWR) Canberra, ACT: Australian Army.

Moir, C, & Dean, J. (2015). A Machine Learning approach to Generic Entity Resolution in support of Cyber Situation Awareness. Paper presented at the Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015).

Moskal, S, Kreider, D, Hays, L, Wheeler, B, Yang, S. J, & Kuhl, M. (2013). Simulating attack behaviors in enterprise networks. Paper presented at the 2013 IEEE Conference on Communications and Network Security (CNS).

Moskal, S, Wheeler, B, Kreider, D, Kuhl, M. E, & Yang, S. J. (2014). Context model fusion for multistage network attack simulation. Paper presented at the 2014 IEEE Military Communications Conference (MILCOM), Baltimore, MD.

Obrst, L. (2010). Ontological Architectures. In Theory and Applications of Ontology : Computer Applications (pp. 27-66), Dordrecht: Springer.

Ormrod, D. (2014a). The Coordination of Cyber and Kinetic Deception for Operational Effect: Attacking the C4ISR Interface. Paper presented at the 2014 IEEE Military Communications Conference, Baltimore, MD, USA.

Ormrod, D. (2014b). A 'Wicked Problem' - Predicting SoS behaviour in Tactical Land Combat with Compromised C4ISR. Paper presented at the 9th International Conference on System of Systems Engineering (SOSE), Adelaide, Australia.

Ormrod, D, Turnbull, B, & O'Sullivan, K. (2015). Systems of Systems: Cyber Effects Simulation Ontology. Paper In Press, Accepted for 2015 Winter Simulation Conference, Huntington Beach, CA.

OWL Working Group (2012). Web Ontology Language, World Wide Web Consortium.

Phillips, C., & Swiler, L. P. (1998). A graph-based system for network-vulnerability analysis. Paper presented at the 1998 workshop on New security paradigms, Charlottesville, Virginia, USA.

RDF Working Group (2014a). Resource Description Framework. Retrieved 18 October 2015, from https://www.w3.org/RDF/

RDF Working Group. (2014b). RDF 1.1 Turtle. Terse RDF Triple Language. Retrieved 18 October, 2015, from http://www.w3.org/TR/turtle/Group

Scott, M. (2013). Operating in a Degraded Information Environment. Australian Defence Force Journal(190), 112-119.

SentinelOne. (2015). Next Generation Endpoint Protection. Retrieved 18 October, 2015, from http://www.sentinelone.com/

Sheyner, O., Haines, J., Jha, S., Lippmann, R., & Wing, J. M. (2002). Automated generation and analysis of attack graphs. Paper presented at the 2002 IEEE Symposium on Security and privacy.

SPARQL Working Group (2015). SPARQL Protocol and RDF Query Language 1.1 Recommendation. Retrieved 18 October, 2015, from http://www.w3.org/TR/2013/REC-sparql11-overview-20130321/

Sudit, M, Stotz, A, & Holender, M. (2005). Situational awareness of a coordinated cyber attack. Paper presented at the Defense and Security Symposium.

Sudit, M, Stotz, A., Holender, M, Tagliaferri, W, & Canarelli, K. (2006). Measuring situational awareness and resolving inherent high-level fusion obstacles. Paper presented at the Defense and Security Symposium.

Swiler, L. P, Phillips, C, Ellis, D, & Chakerian, S. (2001). Computer-attack graph generation tool. Paper presented at the DARPA Information Survivability Conference; Exposition II, 2001, (DISCEX'01).

United States Air Force Space Command (2009). The United States Air Force Blueprint for Cyberspace, Colorado Springs, CO.

United States Army. (2013). US Army Report and Message Format. (FM 6-99).Department of the Army, Washington DC. Retrieved from http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm6_99.pdf

United States Army Training and Development Command. (2014). The US Army Operating Concept: Win in a Complex World. (TRADOC Pamphlet 525-3-1). Fort Eustis, Virginia: United States Army.

Uschold, M, & Gruninger, M. (1996). Ontologies: Principles, methods and applications. The knowledge engineering review, 11(02), 93-136.

Wheeler, B. F. (2014). A Computer Network Model for the Evaluation of Moving Target Network Defense Mechanisms. (Master of Science (Computer Engineering) Masters), Rochester Institute Of Technology, Rochester. Retrieved from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=9690&context=theses

Yang, S. J, Stotz, A, Holsopple, J, Sudit, M, & Kuhl, M. (2009). High level information fusion for tracking and projection of multistage cyber attacks. Information Fusion, 10(1), 107-121.