REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
December 2009	Conference Paper Preprint	May 2008 – November 2009

4. TITLE AND SUBTITLE

MISSION IMPACT OF CYBER EVENTS: SCENARIOS AND ONTOLOGY TO EXPRESS THE RELATIONSHIPS BETWEEN CYBER ASSETS, MISSIONS, AND USERS (PREPRINT)

5a. CONTRACT NUMBER
FA8750-08-C-0166

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
65502F

6. AUTHOR(S)

Anita D'Amico, Laurin Buchanan, John Goodall, and Paul Walczak

5d. PROJECT NUMBER
063O

5e. TASK NUMBER
SD

5f. WORK UNIT NUMBER
03

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Secure Decisions Division of Applied Visions, Inc.
7A Harriman Campus Road, Suite 320
Albany, NY 12206

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RIEF
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TP-2010-16

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release; distribution unlimited. PA # 88ABW-2009-5006 Date Cleared: 2-December-2009

13. SUPPLEMENTARY NOTES
This work, resulting in whole or in part from Department of the Air Force contract number FA8750-08-C-0166, has been submitted to the 5th International Conference on Information Warfare and Security to be held in Dayton, OH 8-9 April 2010. If this work is published, the publisher may assert copyright. The United States has for itself and others acting on its behalf an unlimited, paid-up, nonexclusive, irrevocable worldwide license to use, modify, reproduce, release, perform, display, or disclose the work by or on behalf of the Government.

14. ABSTRACT
Awareness of the dependencies between cyber assets, missions and users is critical to assessing the mission impact of cyber attacks and maintaining continuity of business operations. However, there is no systematic method for defining the complex mapping between cyber assets (hardware, software, data), missions and users. This paper reports the results of an interdisciplinary workshop on how to map relationships between cyber assets and the users, missions, business processes and other entities that depend on those assets. The workshop yielded information about types of impact assessment beyond mission and financial analyses; scenarios illustrating the complex relationships between assets, mission and users; and models for expressing those relationships. The results will be used to develop a system that will automatically populate an ontology from commonly available network data and allow computer network defense, information technology and disaster recovery practitioners to query the system for information about the impact of the loss or degradation a cyber asset.

15. SUBJECT TERMS
Cyber Situation Assessment, Cyber Situation Awareness, Cyber Impact Assessment, Cyber Attack Anticipation, Mission to Asset Mapping, Mission Assurance

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	12	George P. Tadda
U	U	U			**19b. TELEPHONE NUMBER** *(Include area code)* N/A

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships between Cyber Assets, Missions and Users

Anita D'Amico, Ph.D.[1], Laurin Buchanan[1], John Goodall, Ph.D. [1], Paul Walczak[2]
[1]Applied Visions, Inc., Secure Decisions Division, Northport, NY USA
[2]Warrior, LLC, Arlington, VA USA
AnitaD@SecureDecisions.avi.com LaurinB@SecureDecisions.avi.com
JohnG@SecureDecisions.avi.com Paul@warriorllc.com

Abstract: Awareness of the dependencies between cyber assets, missions and users is critical to assessing the mission impact of cyber attacks and maintaining continuity of business operations. However, there is no systematic method for defining the complex mapping between cyber assets (hardware, software, data), missions and users. This paper reports the results of an interdisciplinary workshop on how to map relationships between cyber assets and the users, missions, business processes and other entities that depend on those assets. The workshop yielded information about types of impact assessment beyond mission and financial analyses; scenarios illustrating the complex relationships between assets, mission and users; and models for expressing those relationships. The results will be used to develop a system that will automatically populate an ontology from commonly available network data and allow computer network defense, information technology and disaster recovery practitioners to query the system for information about the impact of the loss or degradation a cyber asset.

Two workshops were held: the first focused primarily on mapping relationships between cyber assets, missions and users in commercial operations, and the second workshop focused on military operations. The participants included people whose operational responsibility is to assure the availability of cyber assets for critical missions, and technology providers and researchers in areas related to the mapping of cyber assets to missions. They represented the armed services, intelligence community, small and large businesses, county government, universities, research companies and large systems integrators.

The workshop goals addressed in this paper are: 1) define the types of impacts one needs to assess when a cyber asset is attacked or fails; 2) analyze scenarios that illustrate impacts of a failed cyber asset on missions and users; and 3) model relationships between cyber assets, missions and users.

Keywords: Mission impact; mission assurance; business continuity; ontology; information security; cyber war

1. Introduction

Awareness of the dependencies between cyber assets, missions and users is critical to assessing the impact of cyber attacks and maintaining continuity of business operations during network incidents. Yet, there are no systematic methods for mapping these relationships. Systems administrators in large data centers often do not know the organizational mission of the devices they manage. Sometimes, the only way of learning these dependencies is: "Let's pull the plug and see who calls" (*The Economist,* 2008). There are no automated procedures or tools for mapping these relationships. This lack of contextual information makes it impossible to rapidly and effectively prioritize allocation of cyber assets or assess the impact of network failures or attacks.

Beyond assessing impact in response to a cyber attack, knowledge of dependencies is also required for planning military missions, business operations and disaster recovery. Planners, commanders and business managers need to understand which cyber assets (e.g. network devices, software applications, data) are critical to the execution of their operations.

Underlying these problems is a need to model the complex relationships between cyber assets and the missions and users that depend on them. The goal of the *Camus* (*c*yber *a*ssets, *m*issions and *us*ers) project is to model these relationships and implement a system for automatically populating that model from commonly available network data sources (Goodall, D'Amico and Kopylec, 2009). The model will form the foundation of the Camus system, from which users can query their own populated model to determine:

- Who relies on an attacked or failed asset to perform their job?
- What organizational mission is impacted by an asset's failure?
- What other assets depend on an attacked asset?
- For a specific mission or task, what cyber assets need to be operating reliably?

We wanted to formulate this foundational model using knowledge and operational expertise gathered from those actively engaged in mission impact analysis of cyber events. Towards this end, we held a workshop that brought together government and commercial practitioners in information technology (IT) and security management, technology providers and researchers – all interested in reducing risks to mission-critical network assets. All of the workshop participants shared a common desire to answer the questions: If this device/application/data is attacked or fails, what organizational mission won't get done? What users will be affected?

This paper reports on the workshop process and results of three workshop objectives: 1) define the types of impacts one needs to assess when a cyber asset is attacked or fails; 2) analyze scenarios that illustrate impacts of a failed cyber asset on missions and users; and 3) model relationships between cyber resources, missions and users. These results have been used by our research team to advance the development of the Camus system and can be used by other researchers as we work together to address the critical need for automated impact assessment. Information about the Camus system can be found in Goodall, D'Amico and Kopylec (2009).

2. Method

Two workshops were held: the first focused primarily on mapping relationships between cyber assets, missions and users in commercial operations, and the second workshop focused on military operations. In addition to five facilitators, 36 people participated, the majority in the second workshop. The participants included people with operational responsibility to assure the availability of cyber assets for critical missions, researchers in areas related to the mapping of cyber assets to missions, and developers of technology that can be used in this mapping. They represented the armed services, the intelligence community, small and large businesses, county government, universities, research companies and large systems integrators.

The workshop commenced with a definition of terms to add clarity and precision to our communications. A workshop facilitator led a group discussion on personal experiences with impact assessment using discussion questions listed below, which served to identify types of impact assessment beyond that associated with mission assurance. Next, break-out groups analyzed predefined, hypothetical scenarios by answering a series of questions designed to elicit the type of information needed to perform mission impact analysis. The groups also constructed entity-relationship-attribute (ERA) diagrams that modeled the relationships between cyber assets, missions and users. The workshop team combined these ERA diagrams into a more comprehensive model that mapped these relationships. This combined model was represented as an ontology and presented to the workshop participants for feedback.

Note-takers documented the discussions and models. These notes were reviewed by the workshop facilitators, summarized and shared with the participants at the end of the workshop and through postings on a workshop web site accessible only to the participants. This paper is the first public dissemination of most of the results.

More detailed information about the workshop process is offered below.

2.1 Terminology

The workshop facilitators offered definitions of terms. After considerable discussion, one major modification regarding the distinction between "asset" and "device" was made. Participants agreed to the following terminology:

Network device – Hardware or software (virtual machine) with an IP address. It is a type of cyber asset.

Cyber asset – A broad term that denotes something of value on a computer network. It includes hardware (e.g. workstations, servers, switches), software (e.g. operating systems, applications), and data (e.g. document files, images).

Network service – Combination of one or more ports open to incoming connections to provide a service to clients. Examples: email, printing, Domain Name Service (DNS), File Transfer Protocol (FTP).

Cyber resource – A general term that incorporates a wide variety of components of a cyber infrastructure. It includes cyber assets, network services, storage media, and physical connections.

Cyber capability – A combination of network services and assets that provide users with the ability to perform an action. The term "cyber capability" is at a higher level of abstraction than device, asset, service, or resource. It expresses an operational need in cyber terms. Examples: Near real-time communication is a cyber capability enabled by VoIP, instant messaging, email, and texting. File transfer is a cyber capability enabled by FTP, email attachment, or instant message attachment.

Missions – A combination of tasks to achieve a common goal. For example, "sell network management software" is a mission. "Operate the company" is too broad to be a mission, and "print invoices" is too narrow, but could be considered a task. Another example: "rescue victims of a hurricane" is a mission. "Manage FEMA" is too broad, while "receive calls for assistance" is too narrow.

2.2 Discussion questions

The following questions were designed to elicit information about how impact assessment, in particular mission impact assessment, is performed by the participants.

- For what purpose do you need accurate mapping of network devices to organizational missions and users? Do you map from the bottom-up (asset to mission) or from the top-down (mission to asset)
- How has the loss of cyber assets affected your operations? What impacts did your organization experience? What and who were affected? What were the cascading effects?
- How do you determine the criticality of a cyber asset?
- What types of impact assessment are you required to do: in response to a compromised or disabled cyber asset; in proactive planning for a failure?
- How do you measure the impact on your critical missions of a specific network asset failing?

2.3 Scenario analysis

Attendees were split into three break-out groups, each with a facilitator and note-taker. Each group was given a setting and asked to analyze various scenarios either working from the top-down or bottom-up. Top-down scenarios were analyzed to answer the question, "If this mission or business process needs to occur without failure, what cyber assets must be fully available?" Bottom-up scenarios were analyzed to identify the specific information needed to answer the question: "If this cyber asset is unavailable, what users and missions are affected?" The commercial and military scenarios were similarly structured, but changed in content to reflect the attendee composition. The commercially-oriented group focused on a bottom-up scenario. We asked the military-oriented groups to first analyze a top-down scenario and then proceed to a bottom-up analysis.

One of the key products of each analysis was an entity-relationship-attribute (ERA) diagram (Daintith 2004) in which missions, tasks, users and various cyber resources are represented as entities; dependencies, physical and logical connections, redundancies and other types of associations are represented as relationships; and the properties of each entity and relationship (e.g. priority) are represented as attributes. We used the resulting ERA diagrams to formulate a larger model in the form of an ontology. We chose ERA diagrams as they are familiar to IT professionals and approximate the form of an ontology without requiring knowledge of ontologies.

Top-down analysis method - Participants started with the mission and worked down to determine the cyber resources upon which it depends, using the steps outlined below.

1. List a sequence of tasks that comprise the mission.

2. List several user roles required to perform those tasks.

3. For a specific task and user role, list the cyber resources and capabilities on which they depend, and any time dependencies.

4. Build an ERA diagram that shows relationships between mission, tasks, cyber entities, and user roles, as well as the attributes of the entities and relationships.

5. List the questions you would ask about each entity and relationship to assure mission completion.

6. Identify sources where electronically-stored data about these entities, relationships or attributes can be found. For example, to find out which devices [entities] connect to [relationship] the database server [entity], we can mine raw network traffic, database logs or a policy control system on the network management system.

Bottom-up analysis method - Participants analyzed the impact of a failed or attacked cyber resource using the steps outlined below.

1. List the various types of impact and how to measure them.

2. Categorize those impacts and select one category of impact for further analysis. Examples are: impacts on mission achievement, morale, loss of lives, revenues.

3. List the questions you would ask about each entity and relationship to assess this impact.

Steps 4 through 6 are shared with the top-down analysis method.

2.4 Scenarios
Groups were given either a commercial or military setting, followed by specific, hypothetical scenarios.

Commercial setting - Sarah Smith is the CIO for a mid-sized financial service firm. The firm houses approximately five hundred employees in a ten-story building. The basement is dedicated to the company's critical data center as well as janitorial services. The company stores and disseminates sensitive financial information for institutions around the world that is accessed 24/7. Downtime of even an hour of the company's website results in lost revenues for the firm and its customers. There is a small network helpdesk and group of network administrators. There are primary and back-up mail and domain servers on location as well as database and web servers that service customers, internal staff and the field sales force. There is a disaster recovery location that can house ten percent of the staff located fifty miles away from the main building. As part of her job, Ms. Smith and her staff must assess the potential effects on the company's business of current network failures, ranging from specific compromised network devices to the loss of network services such as email. She must also schedule maintenance and select courses of action based on the anticipated effects of those activities on her organization's critical business missions and critical users.

Commercial bottom-up scenarios - Ms. Smith has to assess and report on the impact of the following events on the company's ability to provide services to customers around the world:

- A firewall has been mis-configured.

- The CFO's workstation has been compromised by a virus and some sensitive information may have been copied.

- CERTs are reporting a spreading DDoS attack. The IT team has to prepare for the possibility that they will have to shut down traffic coming in through port 80, later in the day or tomorrow.

Military setting - Maj Fibula serves in several roles as a medical doctor, supply officer, and as the 14th Combat Support Hospital (CSH) CIO. He has been deployed along with a Joint Task Force (JTF) to Myanmar to conduct humanitarian assistance operations subsequent to a tropical storm that devastated a large portion of the host nation's geographic area. A mobile network has been stood up to support medical record processing and management of supplies.

The network consists of a number of ruggedized laptop workstations and an HP server. The server hosts: a Microsoft Exchange email server; a Customer Assistance Module (DCAM) application for supply inventory; and MedDecisionDB, an application for managing patient health records. There is a VPN tunnel established from the mobile network through the JTF network to communicate back to the command's sustaining base, where soldier's medical records are archived. The network also provides voice and video capabilities. Below is an overview of the network topology (Figure 1).
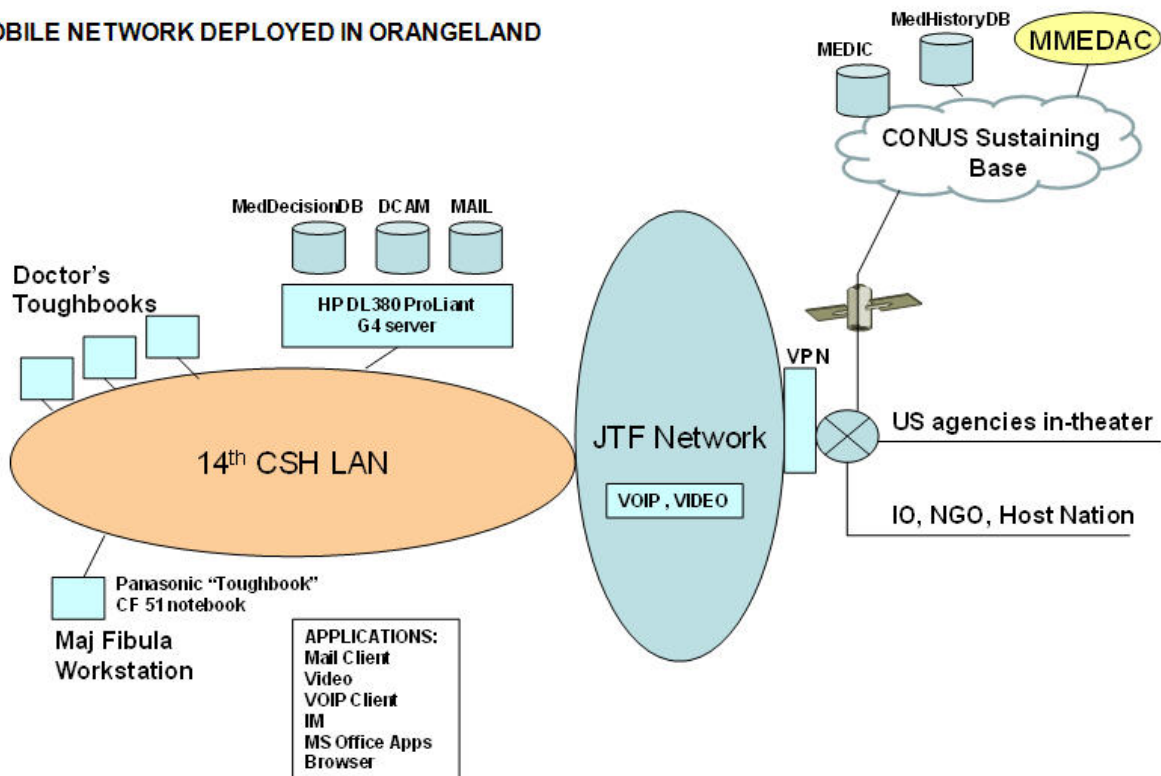

Figure 1: Network for military scenarios

Military top-down scenarios - Participants were asked to select one of the following scenarios for further analysis:

- All JTF forces have to be properly vaccinated over the next few days. Maj Fibula needs to ensure that the needed resources to identify, order and administer needed inoculations are available, and that the medical records of individual soldiers are accessible. What cyber resources does Maj Fibula need to ensure are available and functional?

- The Commander of 1st MEDCOM who is back in CONUS needs to maintain situation awareness of forces in the region, including status of supplies, location of personnel and progress of mission. What cyber resources does Maj Fibula need to ensure are available and functional?

- Doctors at the hospital need to communicate with preventative care experts back in the US tomorrow via video feed. What cyber resources does Maj Fibula need to ensure are available and functional?

Military bottom-up scenarios - Participants selected the type of impact, then assessed that impact within one of the following bottom-up scenarios.

- A firewall was misconfigured in the JTF network, disabling the VPN tunnel.

- The Microsoft Exchange server crashes after applying software updates (patches) and requires maintenance that will take at least four hours to fix.

- A doctor's laptop is found to be infected with malware. Sensitive patient data and medical records of soldiers and staff have potentially been copied to an unknown location.

3. Results

3.1 Types of impact assessment
Participants were asked to discuss the types of impact assessment they perform in response to an attacked or failed cyber asset, and in planning for a network failure. The commercially oriented participants spent far more time discussing various types of impact, compared to the military group, which was oriented towards mission impact. The commercial participants offered 28 different types of impact, which we summarized into the following categories:

Internal Users - This category of impact includes both the productivity of both in-house and mobile corporate users, and issues of general company morale that can result from an incident.

External Users - Customers, suppliers and partners are all external users.

Dependent Assets, Services, and Capabilities - What cyber assets or capabilities will be negatively impacted by the loss any given device? Understanding this impact was central to the workshop and remains a focus of the Camus project.

Level of Severity - Participants' discussion of fixes, workarounds and redundancy revealed that there are different levels of severity for the impact from any incident. The service provided may not be completely lost but only degraded, or the outage is at a time when there is minimal impact, e.g. after business hours. If workarounds or redundant capabilities exist, impact may be minimized.

Revenues - Financial impacts were not directly addressed by the workshop. Identifying which cyber assets are required for revenue-generating activities, however, would bring significant awareness to incident response decisions for commercial enterprises, and also as part of the business continuity, capacity and maintenance planning processes.

Legal/Compliance - Many organizations have contractual obligations or internal/external Service Level Agreements (SLAs) that require systems to be available at specific times or with guaranteed uptimes. Also, some organizations have regulatory requirements regarding how data transactions must be processed (time restrictions, non-repudiation, etc.).

3.2 Results of the scenario analysis
The scenario setting and descriptions were considered realistic. Each of the commercial participants said they had personal experience with one or more of the situations described in the scenarios. Military participants were offered an opportunity to revise the scenarios to more realistically illustrate a mission impact problem; only small word changes were offered.

All three break-out groups in the military-oriented workshop analyzed at least one military top-down scenario. One group completed both top-down and bottom-up scenarios and adhered to the steps of the analysis procedures; a second group completed the top-down scenario using all the prescribed steps except for the sixth step about the data sources; and a third group analyzed the top-down scenario without adhering to the prescribed procedure or answering all the questions. Despite these differences, results were similar.

3.2.1 Entities needed for mission impact analysis
The three groups' ERA diagrams shared many common entities and relationships. All entities except for "applications" and "data" were identified by all three groups. Table 1 presents the entities and examples of each. All groups identified critical tasks associated with administration of vaccines, record-keeping and reporting. These latter two tasks rely heavily on the reliable recording and movement of information.

Table 1: Entities needed for mission impact analysis

Entity	Examples from top-down scenario
Mission	Mitigate spread of new disease; Vaccinate troops and citizens
Task	Access medical records; Order vaccines; Administer shots; Update medical records; Contact CDC; Communicate with soldiers through headquarters; Report progress
User or Actor	Medical administrator; Pharmacist; Shot giver; Doctor; Local commander; Theater commander; Chief medical officer; Soldiers
Capability	VPN access; voice communication; text communication; electronic access to records; secure connectivity
Service	VoIP; smtp; instant messaging; DNS, http
Application	VPN client; Microsoft Outlook; browser; MS Office
Device	workstation; VoIP phone; VPN device; Proliant server; printer; email server; Doctor's workstation
Data	Staff roster; vaccine inventory; staff medical records

3.2.2 Information requirements for mission assurance
The scenario analysis process required that participants identify the questions they would need to have answered about each entity and relationship to ensure mission completion. These questions reflect the information required for mission assurance. Below are examples of those questions.

Doctor's Workstation: Powered on? NIC installed/working? Connected physically to network? Is IP address assigned? Logged in?

Email service: Mail service functional? Can users log in? Can unauthorized users get in?

Outlook application: Is application installed properly? Is it configured to point to proper sendmail server? Have authorized users been identified? Is it tested and working? Is there sufficient disk space for application and data? Is there network connectivity? Is there a valid license for the application?

User – Chief Medical Doctor: Does he know how to use the resource? Is he authorized to use it? Is he authenticated? Can user access the required data?

HTTP Service: Does he have browser? Patch of browser? Availability to port 80? Localhost firewall rules? Tracking cookies or hosts visited? Privileges of browser? What certificates are required?

VoIP Service: Present status, including load, activity and capacity? When was configuration last loaded, how and by whom? Is there a report regarding past performance? Is there an alert mechanism if service fails? What is the Standard Operating Procedure for troubleshooting?

3.3 Ontology

The ERA diagrams and definitions that resulted from the workshop were analyzed and synthesized to bring common elements together. This common structure formed the basis of the resulting domain model, shown in Figure 2. This model has been implemented in OWL, the web ontology language. The ontology continues to evolve as we gather feedback from the workshop participants and other experts.
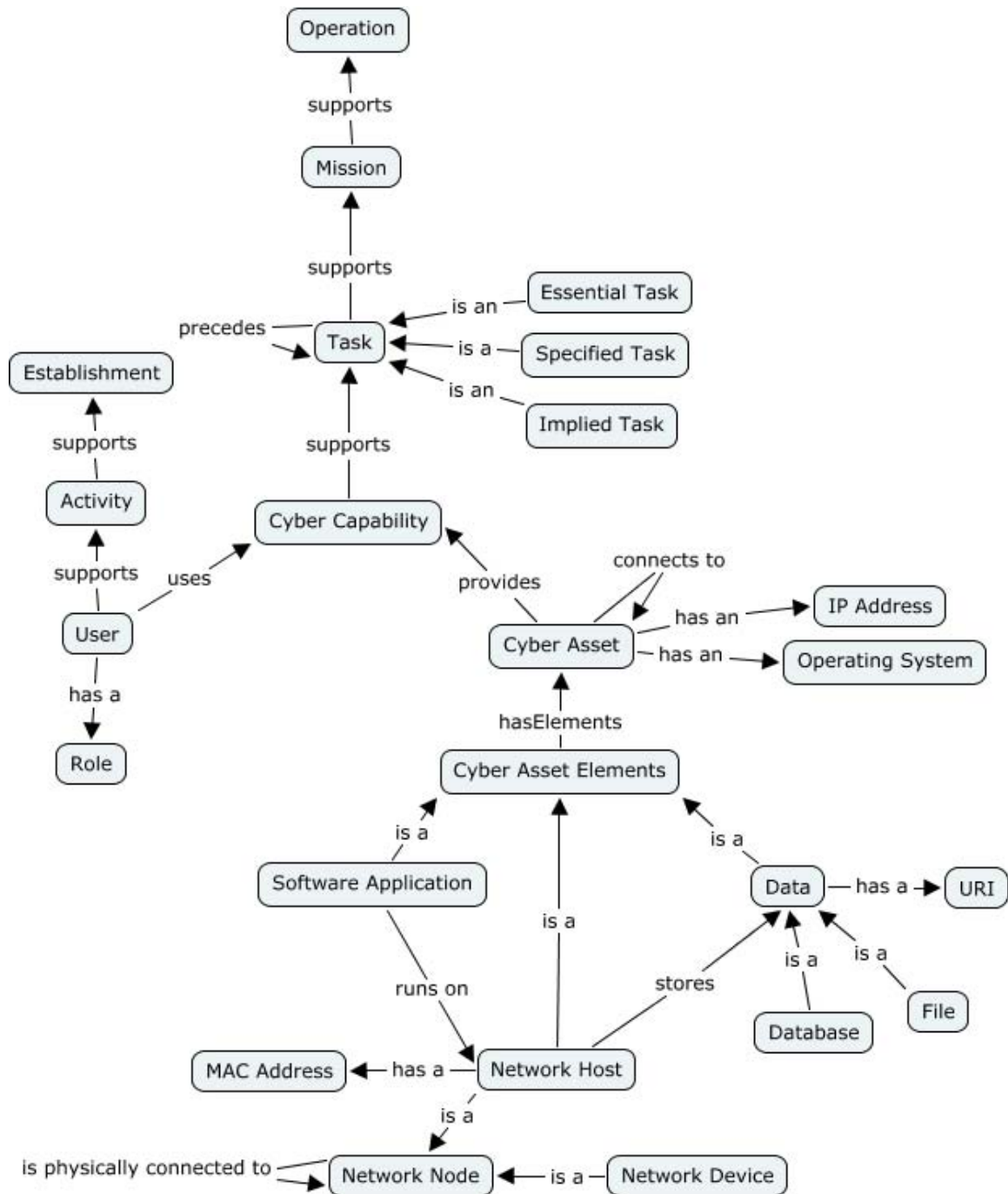

Figure 2: Ontology from workshop scenario analysis

Each domain object, or class, of the ontology is shown in Figure 2 as a node, and links between two nodes define the relationship, or property. The 'is a' property defines a hierarchical relationship; for example, 'software applications', 'network hosts' and 'data' are all subclasses of 'cyber asset elements'. Some properties point from a class to itself, indicating that one instance of that class has a relationship with another instance of that class; for example, one 'cyber asset' may 'connect to' another 'cyber asset'. The top section of the model deals with mission, the left side with users, and the lower section with cyber assets. The 'cyber capability' class acts as a bridge between these three groups. The ontology shown here is minimal, defining only the key classes and properties for mission impact. More classes can be layered on top of this ontology as required to answer specific questions related to mission impact. The classes modeled in Figure 2 are defined in Table 2.

Table 2: Definitions of ontology objects

Entity	Definition	Source
Mission	A task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.	DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/
Establishment	An installation, together with its personnel and equipment, organized as an operating entity.	DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/
Activity	A unit, organization, or installation performing a function or mission, e.g., reception center, redistribution center, naval station, naval shipyard.	DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/
Task	A usually assigned piece of work often to be finished within a certain time	Merriam-Webster Dictionary http://www.merriam-webster.com/dictionary/task
Essential Task	A specified or implied task that an organization must perform to accomplish the mission. An essential task is typically included in the mission statement.	DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/
Specified Task	In the context of joint operation planning, a task that is specifically assigned to an organization by its higher headquarters.	DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/
Implied Task	In the context of joint operation planning, a task derived during mission analysis that an organization must perform or prepare to perform to accomplish a specified task or the mission, but which is not stated in the higher headquarters order.	DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/
Capability	An ability to execute a specified course of action.	DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/
User	Individual or (system) process authorized to access an information system.	CNSS 4009 http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
Cyber Asset	Programmable electronic devices and communication networks including hardware, software, and data..	NERC http://www.eia.doe.gov/cneaf/electricity/page/eia411/nercterms.html

Entity	Definition	Source
(Network) Node	In network topology, a terminal of any branch of a network or an interconnection common to two or more branches of a network.	FS-1037C http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm
(Network) Host	Almost any kind of computer, including a centralized mainframe that is a host to its terminals, a server that is host to its clients, or a desktop personal computer (PC) that is host to its peripherals. In network architectures, a client station (user's machine) is also considered a host because it is a source of information to the network	NIST SP 800-44v2 http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP80044v2.pdf
Network Device	Network device refers to an active device on the network that connects or manages network traffic, such as repeaters, hubs, switches, bridges, routers, and gateways.	Defined by the participants of the workshop.
(Software) Application	Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.	CNSS 4009 http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
Data	Distinct pieces of digital information that have been formatted in a specific way.	NIST SP 800-86 http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
File	A collection of information logically grouped into a single entity and referenced by a unique name, such as a filename.	NIST SP 800-86 http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
Database	Information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files.	DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/

4. Conclusions

The workshop scenarios were well received and readily understood by the diverse group of participants. Additional details about network configurations could be defined, but the lack of granular detail in the current scenario mimics the knowledge gaps that often occur during a cyber incident. We believe the scenarios are suitable for use in further research in the field of mission impact or by anyone who wants to do scenario analysis or knowledge elicitation. The scenarios could also be reused as table-top exercises for organizations working to better understand mission impact within their own environment as part of risk analysis and management.

Having a clear understanding of the terminology, particularly definitions of the entities, was critical to the discussion among both participants and researchers. After review by the participants, the initial Camus model did not dramatically change. Some refinements to the model were discovered, particularly regarding the variety of relationships after participants clearly understood the term "cyber capability" as a way to describe a capacity or functionality required by the mission. This also added richer context to the mapping of missions, assets and users, with subtle but significant differences between "uses" and "dependsOn," or between "isBackupfor" and "isRedundantWith."

Modern networks often contain redundancy or multiple channels that provide the same general cyber capability; this is critical information for prioritizing computer or security resources and is relevant for evaluating network centric warfare. Additional research on the different types of relationships and how they are defined is needed in order to develop automated mission impact assessment systems that can locate additional devices and services that provide a needed cyber capability and display this information to users, thereby providing substantial situational awareness and allowing improved decision making in the event of a cyber incident.

Participants emphasized that impact is not simply about loss of revenue or impeding the mission or business process. It is necessary to understand the goals, measures of success, and priority of a specific mission or organization in order to assess the actual impacts and determine which are critical and which are incidental: if there is limited time to complete the mission, any loss of availability may be a critical; for other organizations, uncertainty about the integrity of specific cyber assets after an incident may be the most critical impact. There are also different temporal aspects of mission which also need to be expressed, for example, Payroll happens on the first and fifteenth of every month; an outage in the payroll server on the seventh is not critical, but the outage must be remediated before the next cycle on the fifteenth. How to define these conceptual components of a mission and means of measuring the impact are areas that are not yet well understood by those working in this area.

We are continuing our research into the issues that were raised during the workshop and welcome the opportunity to work with others who are conducting similar or complementary research on impact assessment.

5. Acknowledgements

6. References

Joint Publication 1-02, (2001) "DOD Dictionary of Military and Associated Terms," [online], Amended 19 August 2009, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

Daintith, J. (2004) "ERA diagram," A Dictionary of Computing, [online], Oxford University Press, http://www.encyclopedia.com/doc/1O11-ERAdiagram.html.

The Economist, (2008) "Where the Cloud Meets the Ground," [online], Special Report, Corporate IT, 23 October, http://www.economist.com/surveys/displaystory.cfm?story_id=12411838.

Goodall, J., D'Amico, A., and Kopylec J. (2009) "Camus: Automatically Mapping Cyber Assets to Missions and Users," Paper read at 2009 IEEE Military Communications Conference, Boston, USA, October.