Cyber Terrain Mission Mapping

Tools and Methodologies

Jeffrey Guion
Center for Cyberspace Research
Air Force Institute of Technology
Wright-Patterson AFB, OH

Mark Reith
Center for Cyberspace Research
Air Force Institute of Technology
Wright-Patterson AFB, OH

***Abstract*— The Air Force is shifting its cybersecurity paradigm from an information technology (IT)-centric toward a mission oriented approach. Instead of focusing on how to defend its IT infrastructure, it seeks to provide mission assurance by defending mission relevant cyber terrain so that a mission can execute in a contested environment. In order to be able to actively defend a mission in cyberspace, efforts must be taken to understand and document a mission's dependence on cyberspace and cyber assets. This is known as cyber terrain mission mapping. This paper seeks to define mission mapping and overview methodologies. We also analyze current tools seeking to provide cyber situational awareness through mission mapping and cyber dependency impact analysis and identify existing shortfalls.**

Keywords—cyber mission mapping, cyber key terrain, mission-centric cybersecurity, mission assurance, situational awareness

I. Introduction

The prominent paradigm in cybersecurity is an information technology (IT)-centric approach where IT assets are protected to provide confidentiality, integrity and availability for systems within an organization. However, across large network infrastructures, it is often unfeasible and inefficient to monitor and protect all assets at all times. An emerging paradigm is mission oriented cybersecurity. The goal of mission-centric cybersecurity is the same as cyber mission assurance; to ensure a mission can perform in cyberspace according to intended purpose or plan. Jakobson asserts "the success of protecting IT infrastructure components should be measured by the success of missions that this IT infrastructure is supporting."[1] In cyberspace, the Department of Defense (DoD), government and private industry are constantly under siege by adversaries with intent to capture information and destroy, disrupt, or degrade capabilities.[2] By taking a mission oriented approach, cyber defenders can actively protect a mission's cyber terrain and form cyber-attack resilient missions. Since many mission essential functions (MEFs) rely on cyberspace, there must be a way to ensure these functions can use the cyber systems necessary to be accomplished. Jabbour and Muccio outlines a 4-step process for cyber mission assurance:[3] 1) Develop and prioritize a list of MEFs 2) Mission mapping to identifying all dependencies a mission has on cyberspace 3) Identify vulnerable assets 4) Analyze risks and mitigate. This process is similar to MITRE's process for Mission Assurance Engineering:[4] 1) Establish mission priorities 2) Identify mission dependencies on cyber 3) Mission impact analysis 4) Threat susceptibility assessment 5) Cyber risk remediation analysis.

In both mission assurance methodologies, identifying MEFs and mapping a mission's cyber dependencies are the beginning steps. Traditional cybersecurity practices incorporate the vulnerability analysis and risk mitigation steps; however often do not incorporate the deeper understanding of what the cyber assets are used for, since the goal is to protect all terrain. Through this paper, we look in further detail into the cyber terrain mission mapping step. There are a few methodologies used for mission mapping and several tools available with different capabilities we will analyze for use within the United States Air Force (USAF).

II. Cyber Terrain Mission Mapping

The goal of mission mapping is to identify Cyber Key Terrain (CKT) for a mission's execution. Raymond [5] applies the physical key terrain definition from Joint Publication (JP) 1-02, "any locality or area, the seizure or retention of which affords a marked advantage to either combatant", to cyberspace to form the definition: "systems, devices, protocols, data, software, processes, cyber personas, or other network entities, the control of which offers a marked advantage to an attacker or defender." However, unlike physical terrain where key terrain is physical and ownership is usually straightforward; control in cyber terrain is often much less clear; it is malleable and the terrain can logically change rapidly. CKT is the physical and logic elements which an organization cannot effectively complete its mission without. According to United States Cyber Command, CKT is temporal and changes with mission and adversary.[6] In the absence of a mission or adversary, these elements are no longer key terrain. Mission mapping is used to associate cyber terrain with the missions that use it. Schulz [7] notes "mission mapping supports mission assurance by connection these layers of information to identify CKT, the dependencies of the CKT, and the risks associated with the CKT."

In the Air Force, there is currently a shortfall of identifying cyber dependencies associated with mission execution. There is a divide between the operational community responsible for carrying out conventional missions and the cyber community responsible for supporting a mission. The operational community does not typically understand all its complex dependencies on cyberspace and the cyber operators do not always know which cyber assets they maintain and protect support which missions. Mission mapping addresses this problem by increasing transparency and understanding of these

complex relationships. The output from mission mapping can then be used as input to cyber situational awareness, mission risk assessments, mission impact assessments, vulnerability mitigation and active cyber defense planning. The rest of this section we will look through a few prominent mission mapping methodologies.

A. *Functional Mission Analysis (FMA)*

In order to be able to provide active cyber defense to a military operation, you must first be able to understand the mission. This is the approach taken by Functional Mission Analysis (FMA). From JP 5-0 "Mission analysis is used to study the assigned tasks and to identify all other tasks necessary to accomplish a mission."[8] FMA is a military adaption of System-Theoretic Process Analysis for Security (STPA-Sec) applied in the cyber operations arena. STPA-Sec advocates taking a top down approach to looking at the cybersecurity of complex systems and critical infrastructure.[9] Most current IT-centric cyber defense methodologies look at cybersecurity from a tactical level. Observing specific threats and vulnerabilities and applying mitigations to them. STPA-Sec applies systems theory, where a system is a hierarchical structure, each level enforcing constraints on the next lower level. This method allows us to approach security as a top down process and apply mitigation to effects rather than causes. FMA applies this system engineering approach to military operations. The highest level is the mission, which forces constraints on the supporting information systems and supporting cyber infrastructure. Using FMA, we can answer the question, what parts of cyberspace, if disrupted, degraded or destroyed by an adversary, can result in unacceptable losses for a mission owner. [10] This is the mission essential cyber terrain or CKT.

FMA is used to build a functional control structure model for the analyzed mission. This control structure model identifies the basic control loop of control actions directed to a system and expected feedback to visualize a system and its dependencies as a controlled process. From this control loop, the individuals applying FMA come up with hazardous conditions which could occur to cause the control loop to fail. These are vulnerabilities to a mission which should be constrained to mitigate risk. The entire FMA process addresses all four steps of the Jabbour, Muccio cyber mission assurance methodology.

B. *Crown Jewels Analysis*

Crown Jewels Analysis (CJA) is a step in the MITRE Mission Assurance process; it is a method for identifying critical cyber assets to an organization's mission.[11] CJA assigns value to IT assets in the context of a mission. It requires an understanding of the IT assets used by an organization and how it is used for a mission. It then estimates the importance of assets by simulating cyber-attacks and modeling their effects to a mission. The cyber mission model must be able to predict the impact of effects to any IT asset to a mission based on organization workflow, activities and relationships. Once the model exists, it uses basic computation to determine a mission's crown jewels or key terrain.

C. *Ontology Modeling*

Secure Decisions Division proposed a ontology-based semantic approach to modeling relationships between cyber assets and the missions and users that depend on them.[12] An ontology model is essentially an entity-relationship-attribute (ERA) diagram with users, missions, cyber capabilities and cyber assets representing the entities which are nodes and the relationships between them as edges. The relationships are expressed as "uses", "depends on" and "requires" to identify significance. Using this representation, a mission can either be described from the top down, "What cyber assets are needed to execute my mission", or the bottom-up, "what missions are impacted by the loss of this system".[13]

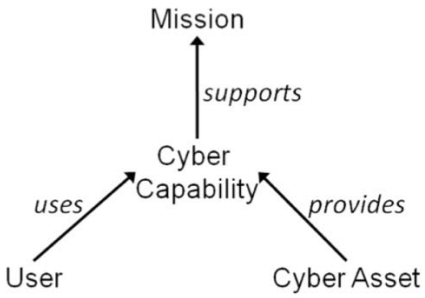

Figure 1. Ontology modeling [11]

D. *Impact Dependency Graph (IDG)*

An impact dependency graph is "a mathematical abstraction of the domain semantics of assets, services, mission steps and missions and all their dependencies."[14] Jakobson uses these to formally describe a mission structure and its cyber terrain.[1] A mission is represented as a sequence or combination of mission steps. These steps then have dependencies on cyber services and assets which may depend on other services and assets. Similar to an ERA diagram, an IDG expresses the missions, mission steps, services and assets as nodes and the dependencies among nodes as edges. If a cyber incident occurs, there is a logical process of mission impact assessment. First detection of the attack or incident and operational capacity impact to the targeted cyber asset. Then the impact will propagate through the IDG cyber terrain up to the top-level mission node and any sequential mission steps where the impact to specific dependent mission steps would be identified.

An extension of the IDG is the time-dependent IDG. This approach adds a time element over the mission-oriented network model. The goal is to be able to capture the temporal characteristics of the mission environment [15]. It uses hierarchical Petri Nets, abstract formal models of information flow[16], to graph a mission's execution. In mission-centric cybersecurity, if an adverse effect of a cyber attack on a victim's machine can be eliminated before it is needed by a mission; it does not have mission impact. This implies a mission's representation should include timing or duration of events and tasks.[15]

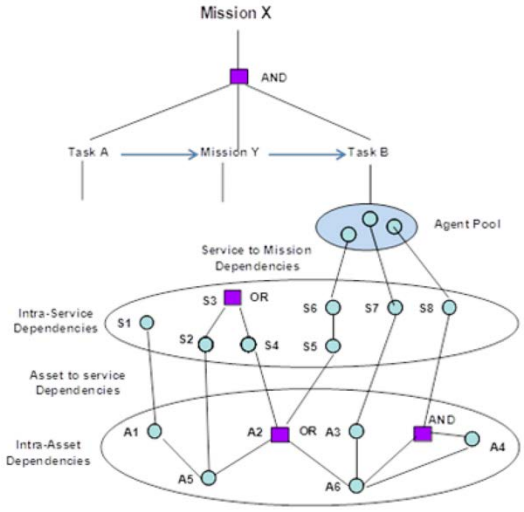

Figure 2. Impact Dependency Graphs

E. Dynamic Mission Mapping

Dynamic mission mapping is an approach to address the shortfall of the static nature of most mission mapping and CKT identification representations. It uses any mission mapping methodology to collect the mission dependencies then integrates information from mission planners, cyber defenders and system owners together on a per mission basis to present a more transparent relationship between an executing mission and its cyber dependencies. Mission planners identify when a mission is executing and which cyber assets it depends on. Any dependencies from those systems to other systems, networks or infrastructure are collected in the static mission mapping step. This information is shared with a cyber defense team so that they have situational awareness on which systems and links are important and need to be protected at which time. Missions are also shared with system owners so they know what missions depend on systems they are responsible for maintaining. This is used to deconflict service interruptions and enhance communication if an outage or incident were to occur.[17]

F. Summary

It's clear from reviewing the mission mapping methodologies, we need a way to decompose and model a mission down to its cyber dependencies. This typically consists of a hierarchical graph or tree structure with mission & MEFs at top nodes, then systems, networks, cyber & physical infrastructure. Dependencies are captured through edges. We also need a way to conduct mission impact analysis for cyber events. In order to have an automated method to conduct impact analysis, each system must have an impact on a mission if system is degraded which propagates up to the mission. CKT is the set of highest impact systems and nodes which could cause mission failure if not available. One additional piece is capturing critical information flows between systems and mission tasks. Although cyber mission impact assessments are often viewed in terms of availability of a system for that mission, the loss of confidentiality and integrity of data within a system could cause mission impacts as well.

III. Cyber Situational Awareness

Once we can model a mission's dependencies on cyber; we must be able to utilize that model for the mission mapping process to be beneficial. In a wide review of literature on cyber situational awareness, Franke found that most literature is concentrated on gathering data from cyber sensors to provide understanding of cyber issues.[18] The literature does not cover in detail how cyber situational awareness can contribute to multi-domain operations. We view the mission mapping process as a way for cyber defenders to understand mission threads so they can identify risks and guide sensor placement to defend key terrain. Data from sensors and monitoring CKT for a mission will provide real time situation awareness for active cyber defense.

There are two prominent approaches to cyber situational awareness.[19] The pioneer of situational awareness for decision making is Dr. Mica Endsley. Endsley's model of situational awareness in dynamic decision making and definitions on SA have become a standard which much future work was built on. Endsley defines situational awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."[20] The key terms defining situational awareness being perception, comprehension and projection. Situational awareness, decision making and action performance are also separated into three distinct stages of the model. Tadda correlates these three stages to the Boyd's OODA loop, situational awareness relating to observe and orient, decision making to decide and performance to act. [21] This model forms a top-down decision process which a person's goals influence which aspects of the environment develop situational awareness.

The second prominent model is the Joint Directors of Laboratories (JDL) model which fuses data from many sources together. This relies on a bottom up approach of using sensors to collect information which is gathered and merged together by sensor management, tracking and identification systems and plotted on a map or visually depicted for the user to comprehend the data.[22]

Much cyber situational awareness literature focuses on gathering data from various sensors such as firewalls, intrusion detection system logs or other high volume sensors and fuse the data to paint a picture of overall cybersecurity awareness. This fits well with the JDL model bottom-up approach. Cyber terrain mission mapping information can be used to build a top-down approach with the high levels being a mission and the lower levels being the systems and dependencies which need to be observed and comprehended to make decisions. Using a top-down mission model, we can determine if a cyber event occurs, what aspect of my mission or business does it impact.

IV. Tools

There are currently some available tools to conduct cyber terrain mission mapping. The purpose of these tools is to provide cyberspace situational awareness and mission assurance by mapping out mission dependencies, identifying CKT and provide impact analysis to a mission. These tools attempt to solve very similar problems but have taken different approaches.

The key areas we will look at are model building, dependency & impact analysis, data sources and visualization.

A. Dagger

Dagger is a modeling framework and visualization tool that seeks to address the problem of cyber situational awareness.[24] Dagger takes a decentralized approach; the application is deployed as a standalone Java application. The users build a layered model to represent their organization's mission. The typical model is the Joint Architecture Reference Model (JARM) 10-layer model, although the layers are customizable. In this model, the top level is the mission and operational drivers, the middle layers are specific applications and services used by the operations and the lower models are networks and infrastructure. Each object in the model is an entity which contains a name, layer (object type), status and dependencies. Higher layers typically depend on lower layers. If the status of a lower layer changes, it propagates up through its dependencies based on a status expression that can be entered or computed automatically based on importance of each dependency. Dagger can also listen through a socket or API to custom data feeds which update an object's status information. Dagger displays its model with each layer being composed of color-coded rectangles representing the individual entities. Dependencies can be viewed by hovering over an entity or clicking it to bring up a sunburst or layered graphic of the entity and its dependencies. Figure 3 is a sample model from Dagger of how phone services impact ability to execute national command authority and provide communications to senior leadership. In this scenario, the cellular network is down and Satellite communications (Satcom) is degraded which severely degrades the iPad, Smartphones and Satcom phones, indicated by the red objects, but only partially degrades the overall missions which are a lighter shade of green.

Dagger is the most straightforward of the tool surveyed. Its functionality can be used from one window. However, it is technical to configure. The basic features such as adding entities to layers and associating dependencies is straightforward but it has advanced features such as creating custom entity status expressions, adding custom indicators to entities, creating data feeds and creating custom what-if scenarios which are more challenging to configure and use. With a layered visualization approach, dependencies are not immediately visible, compared to a graph or tree, unless you hover over or click an object. This approach can do a good job at representing smaller, well defined mission sets but would not scale well on a large mission set with hundreds of dependencies.

We've spoken with a few members of Air Force Cyber Protection Teams that have used Dagger. They expressed the visualization is not sufficient to display to the mission owner that they conduct a cyber risk assessment on. Since the views aren't customizable, besides the ability to show or hide layers, the image you show a mission owner is the same as the view a cyber operator would see. The mission owner doesn't usually have a cyber background to make out what all the boxes mean. The color coded approch does make it easier to explain that those are problem areas but the relationships aren't immediately clear, especially if the cyber operator is building a report which would only include a printout from the tool. An abstracted view tailored to a mission owner about their mission and tasks with details on demand would better address that need.

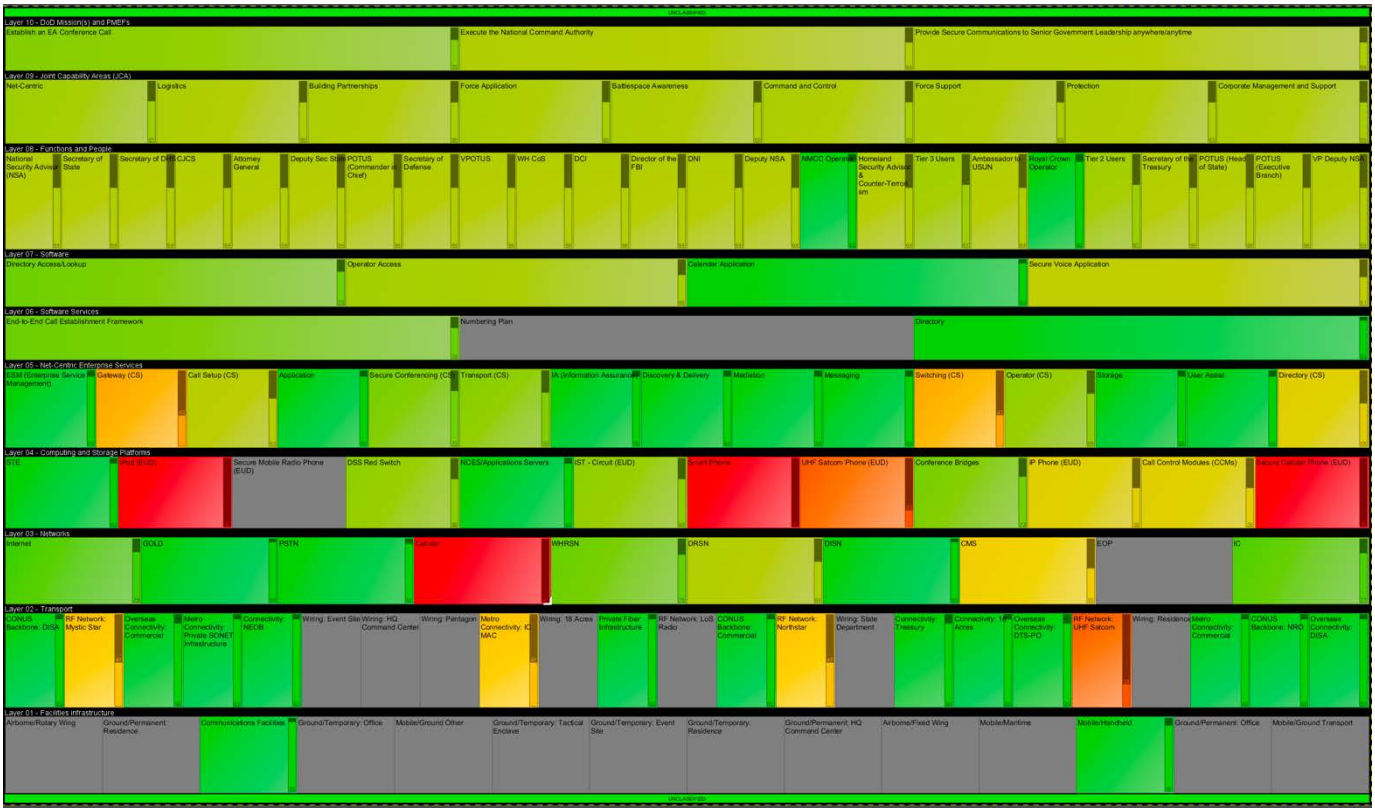

Figure 3. Dagger

Dagger is designed to mainly indicate how system availability impacts missions. However, with a standalone application, it may be difficult to accurately gather status data from the different entities. The user can attempt to create data feeds for different entitites but it is not always possible, especially at the transport and physical layer or the network layer if the devices are behind a firewall. In the case where data feeds cannot be configured, the user would manually have to update the status on an entity which would be challenging to keep timely and accurate. If it was a centralized web service and roles were configured, then a system owner could log in and update the status of their device. Additionally, availability isn't the only important attribute of a dependency. If using Dagger to try to conduct a cyber risk assessment for a mission, the application cannot tell you much more than how the status of a system is affecting, or may affect, mission functions. This information is valuable, especially the what-if analysis can help identify single points of failure or important cyber terrain assets. However, risks to mission are more than just what is the status of these dependencies. There is not a way to input vulnerability information or potential threat information.

B. *Cyber Command System (CyCS)*

CyCS is a MITRE proof-of-concept cyber situational awareness tool. It attempts to improve mission assurance by "enabling the mapping of mission operations to the network operations that support those missions."[25] It builds of the MITRE mission assurance engineering and Crown Jewel Analysis methodology to create a mission model. Mission dependencies are captured through functional decomposition of a mission. The decomposition forms a tree which each parent node depends on its children. The top level of the node being a mission and MEFs and it goes down to capability, service, system, network and circuit. The tree levels are customizable. CyCS also has a dashboard for each entity which can display a mission with its status and CKT or a system with which missions depend on it and the impact it may cause if its status is degraded. Degradations to systems can be entered in the form of a situation. If a situation occurs, it affects a specific object and its effects can propagate up to the mission depending on criticality of that asset. Figure 4 is the CyCS tree view for a mission. In this scenario, a situation is occurring to System 6 which is taking the system offline. The impact of this propagates up to System 4, System 1, MEF 1 and Mission 1. System 4 is red since it has a critical dependency on System 6, but System 1 and its dependencies are yellow since it's dependency is not critical.

CyCS represents a mission with its dependencies most clearly as a tree. It also gives the user several other ways to display the data, as layers, a graph, sunburst or a treemap but these views lack the clarity of a tree graph. Providing a few of the other views such as CKT dashboards are a good way to abstract information and provide details on demand. One drawback of all the proposed tools is they all require a lot of user input to create the mission dependency models. Interviews with subject matter experts is a key requirement for all these tools which takes coordination, collaboration and resources.

Object in CyCS can have custom attributes, for example, confidentiality, integrity and availability. When creating situations, you can select which attributes the event impacts. This begins to touch on the fact availability isn't the only important attribute of a dependency but the capability isn't fully functional in the application. Also, CyCS does not have any built in data sources or capability to accept real time data feeds so any cyber event information which impacts an object has to be entered manually.

C. *Mission Assurance Decision Support System (MADSS)*

MADSS is a DoD cyber situational awareness tool focused on mission mapping and DoD Information Network (DoDIN) operations. MADSS is a web application with a suite of tools providing mission mapping, CKT viewing, mission impact assessments and geo-cyber maps. It supports mission decomposition from a top-down or bottom-up approach meaning objects can be created and can exist without higher or lower level dependencies. The objects are Missions/MEFs, organization/locations, systems, nodes/circuits and physical infrastructure. These objects are linked together with associations where a lower level can specify an impact to a higher level. MADSS offers the capability to quickly build mission models through a mission decomposition wizard which helps walk through the mission mapping process step by step. Although it still requires a lot of manual data collection and input, this is a good way to help guide the user to building the model. MADSS integrates several near real-time data sources to gather information on alerts, trouble tickets, threats, incidents, vulnerabilities, authorized service interruptions from DoD sources which can be associated with different objects to pull status information. Collecting and integrating this information raises the classification of the system. MADSS uses a color-coded tabular representation of data to show CKT to a mission or organization. If the status of a system or circuit changes, it can will update the mission and organization objects with a red or yellow box to show a degradation. MADSS also offers the capability to create formal mission impact assessments through a manual assessment process.

MADSS is designed as an enterprise solution to provide a DoDIN operational picture. It pulls data from several

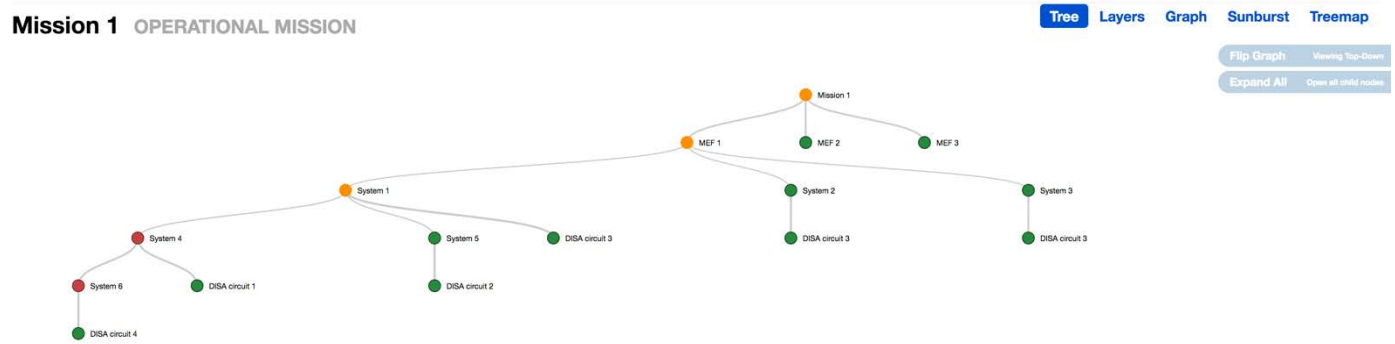

Figure 4. CyCS

authoritative data sources and allows objects to be shared among missions across the DoD. However, it has a problem organizing and presenting information. Although mission models can be built as a tree through the mission decomposition wizard, the CKT views present the information as groups of tables making the information hard to track. Like Dagger, this is not a good way to present information to a mission owner. Since objects are shared across the enterprise, users must search all objects for what they are looking for which creates challenges of finding the correct object to create an association to or know whether a new object must be created. The capability for user roles and data tagging is not built in which are important for enterprise level data displays. Additionally, MADSS requires a large amount of data entry. While this can be beneficial for collecting information on systems and missions, it has the disadvantage of taking a lot of time to gather and input the required information. The mission impact assessment feature has to be generated manually instead of being automatically generated based on the status of an object and its associations to other objects.

D. Cyber Assets to Missions and Users (Camus)

Camus was one of the pioneering proof-of-concept tools for cyber situation management with mission to system mapping capabilities. The modeling framework used in Camus is based on Salerno's Air Force Situational Awareness Model.[19] Camus uses ERA ontology modeling to represent missions, cyber capabilities, users, cyber assets and their relationships.[26] The tool is designed to be able to take raw, structured data sources such as logs or alerts and fuse them together to create ontology instances. This provides a semi-automatic way of forming mission models based on data already on the network. Camus attempted to address the problem of having to collect a lot of data manually with an automatic ontology model generation but was not rolled out for operational testing.

E. Comparison

All the tools have similarities in that they can all create a mission models and associate dependencies down to cyber assets. They all use some form of stoplight color coded objects to represent status to entities based on impact calculations. Dependencies lower in the stack propagate up and impact the mission. The differences between the tools lead to their strengths and weaknesses.

Dagger works best on a smaller mission set where the cyber defenders have control over the majority of the dependencies. In this case, it is easier to create data feeds which update the status of entities in real time. If any changes to the status occurs, the cyber operator can quickly determine potential mission impact of the event. The opposite end, MADSS has the best enterprise capabilities. It is already in use across the DoD. The benefit of an enterprise solution is it helps prevent redundant work. Creating mission models takes a lot of effort, on the scale of weeks. If objects are reused across mission models, then it is much easier to view the impact a system has on different missions across many bases. MADSS is linked with several DoD data sources which can provide cyber event information to automatically update status of key nodes and circuits. Events can also be inputed manually.

CyCS is a good compromise of the two. It is a web application with capability for object sharing across different missions but but there is currently no shared instance across Air Force units. This creates similar problems to Dagger where redundant efforts are made mapping missions to enterprise systems. However, CyCS currently has the clearest mission map. It can present the information at multiple layers of abstraction which can help the user's view items of most interst to them.

All of the data visualizations have trouble scaling to missions with a large number of dependencies. Both CyCS and MADSS use trees which allow the user to expand or contract nodes to view information important to the user. The tree representation has a problem of redundancy since if two separate nodes have the same dependency, each node would have a duplicate subnode. A directed graph would have two edges pointing to one node rather than edges pointing to separate nodes in the tree. The layers in Dagger can be efficient in using space since it does not have edges but cannot condense information so the visualization would quickly clutter with a large number of dependencies.

F. Shortfalls

There are a few shortfalls which exist throughout all of the applications including capturing temporal aspects of missions, capturing information flows between objects, having user roles and role-based views.

Currently, all the tools surveyed have a very static approach to capturing a mission. A mission is one object which can be decomposed to a set of tasks and a set of dependencies. This lacks sufficient ability to capture the dynamic nature of military missions and the temporal aspect of CKT.[7] CyCS was the only tool which supported adding a start and end time to a mission. However, this field wasn't fully utilized to provide a dynamic mission mapping capability. For example, it would be beneficial if a system view could display what specific times a mission was executing that depended on their system or for the mission execution times to be deconflicted with scheduled system service interruptions. In the mission mapping methodologies literature, Jakobson, Raymond, and Cam emphasize the temporal aspect of CKT.[1], [5], [15] From a mission assurance perspective, cyber assets are only key terrain during mission execution. As long as they are secure and operational during that period of time, the mission can effectively be accomplished. In this mission-centric cybersecurity approach, the cyber defenders must know when a mission is executing and which resources it depends on to better form active defense measures.

All of the tools focused on the relationship between a mission and the cyber assets the mission depended on. None of them had the capability to record what information flowed between mission elements. Often the system or application itself is not the important component of a mission, rather the information displayed or produced by the system. Being able to determine what information artifacts will be affected if a system was to be compromised or unavailable is an important factor of a mission risk assessment. If this information was readily available from the cyber situational awareness tool, it would give the mission planner the information so they can make a timely and informed decision. Additionally, documenting

information flows will help identify information dependencies which are often overlooked by an organization.[27] Often vulnerabilities can be introduced in the connections between systems. These information dependencies are areas that must be protected as well.

As commented on above, all of the tools have standard views throughout the application. However, in a military operation, a cyber situational awareness and mission impact assessment tool would have different stakeholders with different information needs.[17] The mission owners are interested in high level views, what are the risks to their mission and why. The cyber defense operators need to know when a mission is executing and what its CKT is. A system owner may be interested to know when missions are dependent on their system so they can better schedule maintenance activities. Capturing mission mapping data supports all these functions but in order to make an application that is usable to the different stakeholders, views can be tailored to better meet their needs rather than to provide a common set of features. CyCS does the best job at providing different levels of information, each object can have its own dashboard which show levels of dependencies above and below it.

V. Conclusion and Future Work

Cyber mission mapping is an important early step in providing mission assurance in cyberspace. Without understanding how a mission depends on cyberspace, you cannot accurately assign cyber defense resources or determine the impact of cyber events on a mission. Since it requires forming links between operational tasks and underlying technology, it is a typically a manual process which requires input from various subject matter experts. We surveyed existing methodologies and tools to determine the key sets of features of a mission mapping and cyber mission impact assessment tool. We also documented some existing shortfalls that can be addressed.

Future work will continue to design and develop a more dynamic mission mapping solution that will take best practices from existing tools and address the shortfalls to meet the needs of a military environment. We also plan on evaluating the benefits of such a tool as they begin to become used to support cyber defense missions in the USAF.

VI. Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

References

[1] G. Jakobson, “Mission-centricity in cyber security: Architecting cyber attack resilient missions,” *Cyber Confl. (CyCon), 2013 5th Int. Conf.*, pp. 1–18, 2013.

[2] M. Reith, “Forging tomorrow’s air, space, and cyber war fighters: Recommendations for integration and development,” *Air Sp. Power Journal2*, vol. 30, no. 4, pp. 96–107, 2016.

[3] K. Jabbour and S. Muccio, “The Science of Mission Assurance,” *J. Strateg. Secur.*, vol. 4, no. 2, pp. 61–74, 2011.

[4] Mitre, “Cyber Mission Assurance Engineering: A Risk-Based, Threat-Informed Approach to Address Advanced Adversaries,” p. 12, 2013.

[5] D. Raymond, T. Cross, G. Conti, and M. Nowatkowski, “Key terrain in cyberspace: Seeking the high ground,” *Int. Conf. Cyber Conflict, CYCON*, pp. 287–300, 2014.

[6] B. G. G. J. Franz, “Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter,” pp. 1–20, 2012.

[7] M. C. Kotson, “Cyber Network Mission Dependencies,” 2015.

[8] U.S. Joint Forces Command, “JP 5-0, Joint Operation Planning,” *Retrieved from Def. Tech. Inf. …*, no. August, 2011.

[9] W. Young and N. G. Leveson, “Systems Thinking for Safety and Security,” *Proc. 2013 Annu. Comput. Secur. Appl. Conf.*, pp. 1–8, 2013.

[10] C. Mixon, “Functional Mission Analysis (FMA).” Air University, 2016.

[11] S. Musman, M. Tanner, A. Temin, E. Elsaesser, and L. Loren, “A systems engineering approach for crown jewels estimation and mission assurance decision making,” *IEEE SSCI 2011 Symp. Ser. Comput. Intell. - CICS 2011 2011 IEEE Symp. Comput. Intell. Cyber Secur.*, pp. 210–216, 2011.

[12] P. Anita, D’Amico;Buchanan, Laurin; Goodall, John; Walczak, “Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships Between Cyber Assets, Missions and Users,” *2010 Int. Conf. Information-Warfare Secur.*, vol. 298, no. 704, pp. 388–397, 2010.

[13] L. Buchanan, M. Larkin, and A. D’Amico, “Mission assurance proof-of-concept: Mapping dependencies among cyber assets, missions, and users,” *2012 IEEE Int. Conf. Technol. Homel. Secur. HST 2012*, pp. 298–304, 2012.

[14] G. Jakobson, “Mission cyber security situation assessment using impact dependency graphs,” *14th Int. Conf. Inf. Fusion*, pp. 1–8, 2011.

[15] H. Cam and P. Mouallem, “Mission-aware time-dependent cyber asset criticality and resilience,” *Proc. Eighth Annu. Cyber Secur. Inf. Intell. Res. Work. - CSIIRW ’13*, p. 1, 2013.

[16] J. L. Peterson, “Petri Nets,” *PLoS One*, vol. 9, no. 3, pp. 223–252, 1977.

[17] J. Guion and M. Reith, “Dynamic Cyber Mission Mapping,” in *Industrial and Systems Engineering*

Conference, 2017.

[18] U. Franke and J. Brynielsson, “Cyber situational awareness – a systematic review of the literature,” *Comput. Secur.*, vol. 46, p. 41, 2014.

[19] J. J. Salerno, M. L. Hinman, and D. M. Boulware, “A situation awareness model applied to multiple domains,” vol. 5813, pp. 65–74, 2005.

[20] M. R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems,” *Hum. Factors J. Hum. Factors Ergon. Soc.*, vol. 37, no. 1, pp. 32–64, 1995.

[21] S. Jajodia, P. Liu, V. Swarup, and C. Wang, “Cyber situational awareness: Issues and research,” *Adv. Inf. Secur.*, vol. 46, pp. 15–36, 2010.

[22] S. Schreiber-Ehle and W. Koch, “The JDL model of data fusion applied to cyber-defence—A review paper,” *Sens. Data Fusion Trends, …*, no. September, pp. 4–6, 2012.

[23] G. P. Tadda, “Measuring performance of cyber situation awareness systems,” *Proc. 11th Int. Conf. Inf. Fusion, FUSION 2008*, pp. 334–341, 2008.

[24] E. Peterson and J. Ockerman, “Dagger : Modeling and Visualization for Mission Impact Situation Awareness,” 1985.

[25] M. C. Solutions, “An Overview of MITRE Cyber Situational Awareness Solutions,” no. May, pp. 1–17, 2015.

[26] J. R. Goodall, A. D’Amico, and J. K. Kopylec, “Camus: Automatically mapping cyber assets to missions and users,” *Proc. - IEEE Mil. Commun. Conf. MILCOM*, pp. 1–7, 2009.

[27] M. R. Grimaila, L. W. Fortson, and J. L. Sutton, “Design Considerations for a Cyber Incident Mission Impact Assessment (CIMIA) Process,” *Int. Conf. Secur. Manag.*, 2009.