Cyber Mission Mapping

A Proactive Approach to Cyber Mission Assurance

1st Lt Jeffrey Guion
Center for Cyberspace Research,
Air Force Institute of Technology,
Wright-Patterson AFB, OH 45433
jeffrey.guion@afit.edu

Abstract— **The DoD is highly dependent on cyber systems and network infrastructure in order to execute missions and achieve its national defense objectives. It has incorporated the concept of cyber mission assurance, a risk management activity focused on assuring an organization's mission capability in response to loss or degradation of cyber capabilities. However, there exists a disconnect between cyber service providers and the operators that rely on their services. In order for the operational community to better synchronize with the IT community, there must be a way to map a mission's cyber dependencies and deconflict them with those systems' cyber defense and system maintenance activities. We analyze the aforementioned problem and propose a software solution to proactively support mission assurance by mapping a mission down to its cyber assets, identifying system dependencies on resources and its critical infrastructure, and deconflicting missions with system maintenance schedules. The goal is to enhance collaboration and provide a deconfliction and risk analysis mechanism for mission owners and service providers. We created event models to analyze how system maintenance activities impact a given mission. We present architectural designs and evaluation of the proposed solution. These models can be further applied to cyber defense or disaster preparedness activities.**

Keywords: cyber mission assurance; mission mapping

I. INTRODUCTION

Consider the following hypothetical scenario. An Air Operations Center (AOC) is executing a time sensitive targeting mission thread. The mission commander's decision to engage a target depends on the intelligence from a system that receives video surveillance feeds from remotely piloted aircrafts. During the mission, two events suddenly occur:

(1) The intelligence analysts at the AOC are unable to access the video stream for unknown reasons.
(2) The network operations squadron (NOS) supporting the AOC has a report of a denial of service (DoS) attack which is disrupting network traffic.

The mission commander only knows that they do not currently have access to the data they need in order to carry out the mission. The NOS knows there is a cyber attack causing outages but does not know which mission systems rely on the network devices under attack.[1] Event 2 could be replaced with a number of scenarios. The system which intel analysts access the video stream from could crash and is experiencing an unexpected outage; or the system owner could be patching critical vulnerabilities and the outage was planned but the mission commander was never notified. Regardless, there often exists a lack of overall cyberspace situational awareness to all elements that may affect a given mission.

A further problem is when systems do go down, a mission commander may not know who to contact in order to get a status update. A mission typically depends on a set of systems which each depend on their own chain of systems, circuits or network devices. Consider Figure 1. The mission owner for Mission 1 might know they depend on System1 and System 2 in order to execute. What they may not know, is they also depend on System 4, System 5 and System 6. So if System 6 goes down, it will impact System 1, System 4, Mission 1 and Mission 2. However, in System 6's view of the world, only System 4 depends on them. They may not understand when and what missions depend on

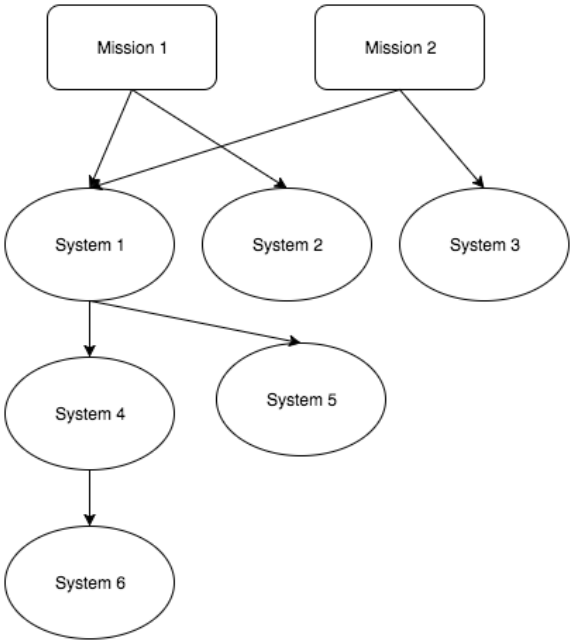

Figure 1: Mission to System mapping

them in order to execute. In the mission owner's view of the world, System 1 is down so I must contact them to fix their issue. There isn't transparency between mission and cyber system dependencies because of lack of visibility and communication between the cyber community and operational community. We propose a software solution to help address this problem.

II. Motivation

As most papers discussing cyber within the military begin; the Department of Defense (DoD) heavily relies it's cyber systems and infrastructure in order to carry out its mission. The net-centric advantages that using information systems for planning, coordination and execution provide also add complexities and broaden attack vectors to the DoD. The cyber environment is contested by adversaries, meaning systems are attacked with intent to destroy, disrupt or degrade capabilities.[2] The domains of land, sea, air, space and cyberspace do not operate independently of one another. Just as space aids in air operations, or air supports land operations, cyberspace effects can easily bleed over to other domains. Without cyber assets, many missions throughout the United States Air Force (USAF) would be significantly degraded, if not reach a complete stand still.[3] Military leaders stress the importance of maintaining the freedom of maneuver in cyberspace. USAF Chief Information Officer (CIO) Lieutenant General William Bender notes "Freedom of action in cyberspace through the application of mission assurance is a prerequisite for successful Air Force core mission execution."[4] For that reason, the concept of cyber mission assurance has been investigated and is currently being pursued by both academia and the Air Force cyber community.

III. Cyber Mission Assurance

DoD Directive 3020.40 defines mission assurance as "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan." [5] Given that most missions throughout every warfare domain have a dependency on cyberspace in order to execute; there must be a process to ensure cyber assets are available when needed and appropriate risk management decisions are taken incorporating cyber vulnerabilities. AFDD 3-12, *Cyberspace Operations,* defines mission assurance with regard to cyberspace as "measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities."[6] There is currently a shortfall within the Air Force and the DoD in following the four tasks to achieve this function.

What does cyber mission assurance look like? Air Force Research Lab senior scientists Dr. Jabbour and Dr. Muccio assert mission assurance requires a four-step process, following the same tasks as outlined in the AFDD 3-12 definition: prioritization, mission mapping, vulnerability assessment, and threat mitigation.[7]

(1) Prioritization is the first step; it requires developing a list of mission essential functions (MEF) and prioritizing them. Prioritization is a risk management activity that requires input from a mission commander in order to determine what the critical elements of a mission are.
(2) Mission mapping is a crucial step to mission assurance. It involves identifying all dependencies a mission has on cyberspace. These dependencies within MEFs are also known as cyber key terrain (CKT). Each mission can be decomposed to components, tasks or functions. The previous step should help determine a prioritization of mission functions which input into the mission mapping. For each MEF, each atomic cyber process should be outlined. Individual system dependencies should be identified and propagated to create a dependency graph. There should also be some rating of system importance to the mission in this step. All DoD information systems are assigned a mission assurance category (MAC) on a scale of I-III which indicates if a system is critical to a warfighter's mission.[8] Ideally this determination would be based on an analytical framework and stakeholder inputs rather than a static MAC.
(3) The first two steps are a necessity in being able to determine how a mission is dependent on cyber assets in order to execute. The next step, vulnerability assessment, is to determine vulnerabilities, threats and vectors for attack towards the cyber assets and information flows. It also should determine single points of failure to critical mission functions. This step requires analysis from cybersecurity professionals and input from vulnerability analysis tools. Here a mission assurance team can determine what the vulnerabilities and threats to each mission process and what the impact on a mission would be if an outage were to occur. Vulnerabilities should be assigned a severity level based on threat and impact which feeds into the next step.
(4) The final step is to analyze risks from the vulnerability analysis and mitigate them to an acceptable level. The goal is to use cybersecurity practices to reduce the exposure to and impact of cyber compromises. This framework provides the data necessary to reduce uncertainty in a cyber environment and more accurately determine risk to a mission from its cyber dependencies.

A survey of existing cyber network mission dependency tools conducted by MIT's Lincoln Labs categorized the tools into two categories: process-driven analysis and artifact-driven analysis.[9]

Process-driven analysis is typically conducted manually by subject matter experts. It requires input from various subject matter experts to identify missions, processes and system dependencies. This is the approach the USAF is currently taking with the Communications Squadron Initiative (CSI) pathfinder. Under the CSI, next generation cyber units would be primarily responsible for cyber mission assurance rather traditional IT services. They would work more closely with the operational units protecting and defending relied upon cyber assets. The pathfinder is a method allowing a sample of units to trial mission assurance techniques and feed findings and results back to the rest of the Air Force for widespread implementation. The drawback of process-driven analysis is it is highly time consuming and complex to attempt to understand and map out a mission's cyber dependencies. Also, the output of this process is determining cyber key terrain and a static mapping of missions to system dependencies. Since it is static, it takes a lot of maintenance to keep up to date and accurate.

An artifact-driven approach uses logs and data from hosts and sensors to map out a network with dependencies. However, this typically will not include information pertaining to specific missions. It also requires tools to be in place to be able to scan a network and gather high fidelity data. Lincoln Labs concluded that neither a process-drive nor an artifact-driven approach will entirely solve the problem and should be a combination of static and automatic analysis.

Another problem with the currently available tools is the level of complexity required to use the tool. The 24th Air Force, Air Forces Cyber, is exploring available mission mapping tools to deploy to units participating in the CSI pathfinder. Direct feedback from these units are the tools are complex to use, labor intensive to input the data manually and the costs have outweighed the perceived benefits. One unit expressed that it was easier to statically map a mission using sticky notes on a wall rather than trying to understand and use these complex tools. The systems are designed for administrators with high technical understanding of network topologies, system relations and an understanding of how operational missions are structured. In a deployment to the USAF, the users would have varying degrees of technical experience and minimal formal training on the tool.

One more interesting observation by Lincoln Labs was that all technologies surveyed only consider chronic mission types, missions that are either executed continually or repeatedly.[9] Missions that are only be executed once or specific occurrences of missions are not taken into consideration. This may be an oversight due to the dynamic nature of military operations. Although cyber defense is a 24/7 commitment, a mission's reliance on cyber is usually not.

Our approach is to integrate mission mapping with the real time scheduling of missions and cyber maintenance activities. The USAF already has a mechanism to schedule operational missions. As outlined AFDD 1, the Air Tasking Order "articulates tasking for joint air, space, and cyberspace operations for a specific period, normally 24 hours. Detailed planning generally begins 72 hours prior to the start of execution to properly assess the progress of operations, anticipate enemy actions, make needed adjustments to strategy, and enable integration of all components' requirements." Part of the planning cycle could include working with a cyber mission assurance team to ensure cyber assets are available. In order to properly perform risk analysis; mission planners must be able to determine the status of the cyber assets that their mission relies upon. However, the operations community is not typically synchronized with the IT community. There is not a formal process where an operator registers to use an electronic service so the service provider knows when their system is being used. This is a problem because when a system goes offline, a system owner often won't know who to notify. With a little collaboration and input from mission mapping process; network friendly fire can be avoided and mission owners can have more visibility into the status of the systems their missions are dependent on. This information is key in performing risk management and data driven decision making.

IV. Technical Approach

We are designing and developing a high level mission mapping application. The primary goal of our application is to offer the USAF a technical solution for de-conflicting system maintenance activities, known as authorized service interruptions (ASIs) with scheduled missions. An ancillary goal is to provide a framework which can be further extended to support functional mission analysis, cyber defense actions and other mission assurance capabilities.

The approach we've taken is to explore a decentralized mission assurance solution. There are many individuals with information required for cyber mission assurance; however each individual only has a piece of the necessary information. Operators know when missions are scheduled and what first level systems they use. A communication's squadron or cyber protection team understands cyber dependencies, information flow and defensive cyber activities. Service owners know how to keep their system's patched and operational. It is rare one organization has end-to-end oversight for all cyber dependencies. Therefore, in order to be able to deliver cyber capabilities, when and where they are needed, collaboration is needed by all participants. Cyber mission assurance is not something created by technical experts alone.[4] The traditional approach to IT services is that the users are customers. Service providers make a best effort to ensure reliability but have little interaction with consumers. This framework is not sufficient in providing services in a contested environment; a greater degree of partnership and resiliency is needed.[2] Similar to maintenance or logistics, IT must

act as mission partners to ensure that systems are available when called upon.

Let's consider the use case of an emergency service interruption. A service owner discovers a critical vulnerability in their system which must be remediated as soon as possible. The service owner should have a way to directly communicate with missions that may be affected by this vulnerability or service interruption. This capability enhances the relationship and provides mission planners the data needed to effectively plan their mission. Currently, those relationships do not exist in most cases. A mission doesn't have its dependencies mapped to a system level and a service owner doesn't know when missions rely on their system. A service provider will have to send a message to all users saying when a system will be taken down or conduct the maintenance and let the users find out the system is down on their own.

Figure 2 is a high level use case diagram for our application. It outlines the actors and interactions between actors and the system. The primary actors are: (1) Mission Planner, (2) Administrator, (3) Service Provider, (4) ASI Manager, (5) Mission Owner.

(1) The mission planner is a member of the operational community that is responsible for scheduling missions and coordinating resources required for that mission. Their goal is to ensure cyber assets are available when needed for the mission. In order for this to be possible, their missions must be registered in the application with the system dependencies mapped out to their mission. For situational awareness, they should be able to view their missions with the current status of any cyber dependencies so they can appropriately conduct risk analysis.

(2) The administrator is member of the IT community charged with cyber mission assurance. This role is typically performed by a USAF communications squadron under the CSI or a cyber protection team. The administrator will initially work with the mission owners and service providers to map out prioritized missions' cyber dependencies. They will then continue the role of coordinating between missions and services maintaining situational awareness of ongoing missions occurring on their base and system status for dependent systems. They will also be responsible for performing vulnerability analysis and mitigation.

(3) The service owner is the system owner that provides an electronic service to a mission. They are responsible for system maintenance & repair activities. They must submit ASI requests for any scheduled system down time and report any outage for their system. Service providers can view missions that rely on their service.

(4) The ASI Manager coordinates and schedules service interruptions requested by service owners. They will send ASI requests out to potentially impacted mission owners, system owners or other affected parties which concur or non-concur with a request. An ASI must not occur until approved by the ASI manager.

(5) The mission owner is the commander with authority over a mission. They are responsible for identifying

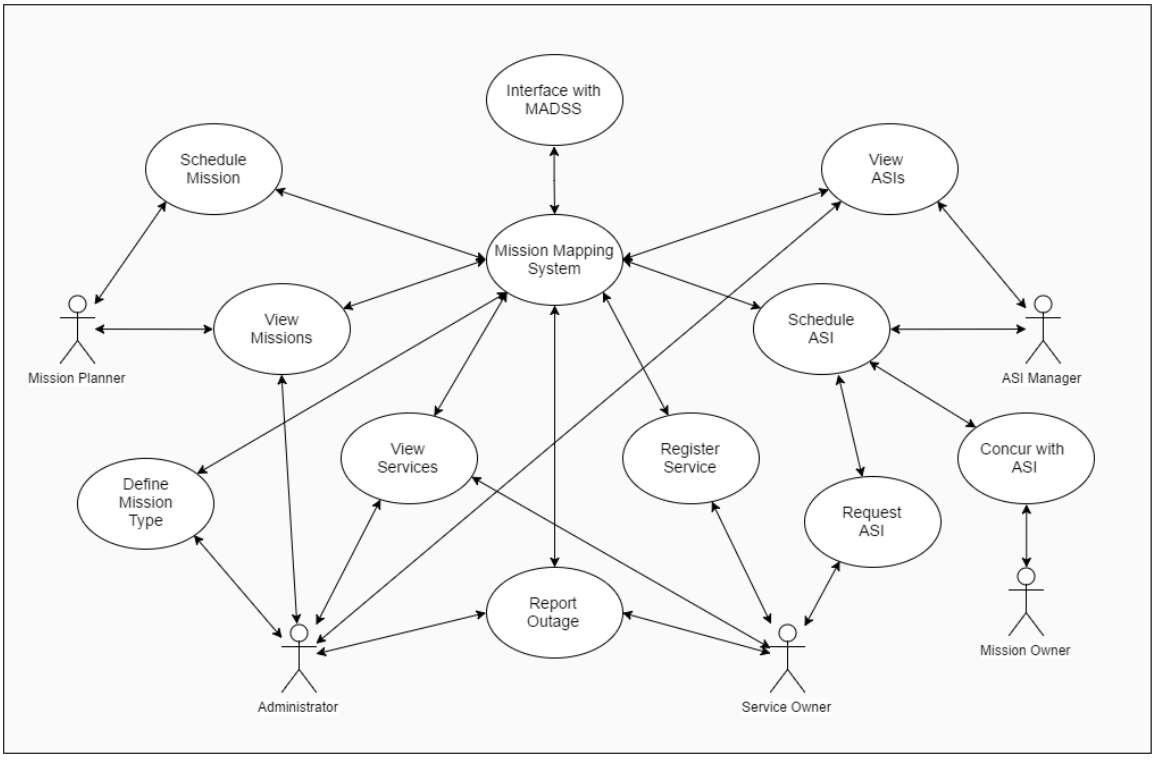

Figure 2: Use Case diagram

mission essential functions, prioritizing missions, risk management and non-concurring with ASI requests if it negatively impacts a given mission.

The application is driven by three major objects, Missions, Services and Service Interruptions. Figure 3 depicts their relationships. Each of these objects have a many-to-many relationship with each other. A mission may depend on many services in order to execute and many different missions may rely on a specific service. A service may undergo many service interruptions, usually occurring on different dates periodically. Additionally, a service interruption may affect many services. For example, maintenance to a network gateway could bring down external access to all systems within its enclave. Lastly, a service interruption can impact multiple missions and a mission can be affected by many service interruptions. Using these simplified object relationships; dependencies can be calculated and displayed in an understandable manner which allows for high level situational awareness by both the operational community and the IT community. Currently, in many situations, neither side has sufficient visibility into the daily operations of the other community. Providing this visibility will give mission planners information to help incorporate cyberspace into risk based decision making and will help the IT service providers become mission partners and working toward mission assurance.

V. ARCHITECTURE

Our mission mapping application falls within a *mission / operational architecture* framework. This architecture describes operational aspects of the model by identifying missions, tasks and their priorities.[10] It also identifies mappings to the technical architecture which include task dependencies on cyber resources. We chose to have an operational viewpoint in order to display actionable data to the users. Colonel Bryant, director of the Task Force Cyber Secure for the AF CIO, notes "Mission assurance in and through cyberspace is not fundamentally an IT problem but a mission problem that requires a mission focus and approaches that go beyond what we have come to think of as traditional cybersecurity."[11] The intent of the application is to provide a mission assurance tool where the views in the tool are all highly mission oriented.

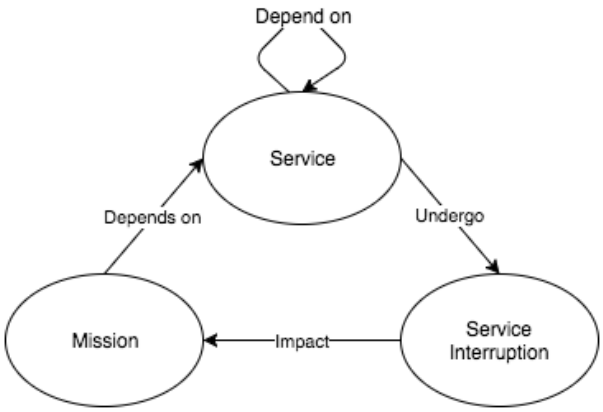

Figure 3: Mission dependencies

The application is a client-server model that follows the model-view-control architectural design pattern.

A. *Model*

System elements such as missions, services and service interruptions are software defined data models. The server hosts the object-relational mapper (ORM) that mediates between the data models and the relational database. This is in order to create an object oriented representation of the data. The model can perform any calculations, manipulations or logic to the data before passing it forward to the view. This is important for the application so dependencies can be calculated based on standard objects.

B. *View*

The views are HTML templates which display the requested data. Having an object oriented model allows for a standardized representation of the data by the front-end application. Since the views are the interface which the user will interact with, they must accurately represent the data and display it in an intuitive, easy to use manner. We will further discuss the views in the next section.

C. *Controller*

Requests are handled by the controller primarily through a URL dispatcher. The client requests the page they would like to view and based on the user's permissions and any input parameters, the model performs any necessary calculations and returns the relevant page. The client can also enter data into the views, such as ASI requests or mission mapping data. This data will then be passed back by the controller to the model to create new or modify existing objects.

One important element of gathering the data required to continuously map missions and maintain timely, accurate information is an element of automated data generation. This can be done by importing data sources from other applications in order to prevent redundant manual input. Our application is designed to interface with the Mission Assurance Decision Support System (MADSS). MADSS is a DoD system designed to provide Combatant Commanders, Services and Agencies enhanced cyberspace situational awareness including the identification of critical risks to supported missions. It's features support mission mapping, critical asset and single point of failure identification, geographic, real time network data monitoring, and an array of other solutions requested by DoD customers.[12] While MADSS has a lot of capabilities; it relies on user inputted, static mission to system mapping. The number of features also makes the system complex for non-administrators to use.

MADSS gathers and displays data through a service-oriented architecture. Each of its data sources are different services that MADSS uses to derive information on missions, systems and their operational status. Our application is designed to leverage that existing data in MADSS and port them into our model to be displayed in our application's views. The data MADSS currently contains includes high level network circuit layouts with system statuses, DoD organizations and real time network events from several authoritative data sources. Our application will add on to these capabilities by providing a mechanism for the user community to conduct mission to system mapping, identify specific mission execution timeframes and view data in intuitive operational views. Complexities in MADSS make it difficult for users to input the necessary information. Since MADSS relies on user-driven content by the services; missions and system dependencies will be exported back into MADSS after inputted into our system. In that way, our application acts as a facade and masks some of those complexities by providing views that are understandable to Air Force users both in the IT community and operational community. Our application still leverages MADSS by importing any service interruptions or real time network event monitoring information to reduce redundancy of manual user input and software engineering efforts. The systems should exchange data through a SOA application program interface (API). The data received from MADSS would then be processed to correspond with our models. The data exported to MADSS would be a service representation of data that MADSS utilizes.

VI. Application

The application is designed for simple crowd-sourcing of mission mapping and system status information. It relies on mission planners scheduling their mission's in the application with connected system dependencies, future iterations will explore automated imports of scheduled missions from existing systems. The mission owner along with a cyber mission assurance team will be able to map out mission types for a unit to create templates for reoccurring missions. This is the static mission mapping step. The data becomes dynamic when the mission planner schedules missions as they occur. Services can be added into the application by the service owner. They will identify the next level dependency their service depends on, be it another system, circuit or base network. Service owners are able to submit authorized service interruption request or input outages and emergency service requests through the application and it will notify affected parties. Also, service providers are able to view which missions depend on their services giving them a greater understanding of requirements for their systems.

The views within the application are based on the major objects, Missions, Services and Service Interruptions. The Missions view will show all scheduled missions for a user. This is where they can schedule upcoming missions or view the details on any scheduled/ongoing missions. If a mission occurs regularly, a template can be created which can populate all the fields and dependencies other than start and end time so missions can be quickly inputted. A user can view details on a mission including those system dependencies and the status of those systems. It is mission oriented so planners can make sure systems are operating as expected giving them cyber situational awareness before and during mission execution.

The Services view displays information on all the services a user has access to view. Here the service owner can add new services, edit existing services, submit ASI requests or input outages. When services are added into the application, they should identify first level dependencies on other services, internal networks or circuits. Degradations to any dependency will be displayed affecting the status of a service. A service owner has the ability to report an outage with expected remediation time which immediately marks their service as degraded. This will automatically notify any effected mission planners or dependent service owners so they can understand the status and can incorporate it into any risk management decisions. Additionally, by viewing details on a service, the service owner can determine which missions are utilizing their service. This can help them determine periods of non-disruption and help quantify a service's importance to mission execution.

The Service Interruption view displays both authorized and pending service interruptions. ASIs show which systems have upcoming scheduled down time. The user can view the impact of the ASI by seeing which other systems it affects, if any. Pending ASIs are displayed to a user if it affects their mission or service. They are able to concur or non-concur with the request and provide a mission impact if they non-concur. This information is sent to ASI Managers for final approval and scheduling of service interruptions.

Although this form of application does require continuous manual user input; it creates an opportunity to increase partnership between the operational and IT community. By understanding a mission's dependence on cyber, the IT service provider has an opportunity to increase the operational scope of their mission. They will understand the mission impact of their system which currently is hard to quantify and communicate. The application also allows cyber mission assurance teams to analyze mission dependencies to determine the most critical assets and key cyber terrain. It helps increase cyber terrain visibility which is important to commanders assigning resources. If the most important systems and links are identified, those are the ones that need the highest degree of protection.

We've attempted to make inputs and interactions with the application simple requiring minimal technical expertise to use. This is to reduce the barrier of entry for the system to be used. Since it requires collaboration from operational units, service providers and communications squadrons;

each of those entities must find benefit in the tool for it to be effective. It's not initially designed as a vulnerability assessment tool but by proactively creating a mechanism for communication, it can help shape a culture of cyber mission assurance.

VII. Conclusion

Cyber mission assurance is a complex problem that is not going to be solved immediately. Our mission mapping application is designed to address a piece of that problem with the mission to system mapping and near real time system status capability. While there are existing tools available with mission to system mapping capabilities, most have the shortfall of requiring a highly granular degree of detail making input laborious and complicated. The DoD has hundreds of military bases around the world which all have many individual missions that depend on cyber assets. Having a complex system with a high degree of technical knowledge is not plausible in all situations. Our application is to provide a simplified approach to mission mapping that can be understood and utilized regardless of training and technical expertise. It relies on collaboration between the operational community and cyber community in order to be effective. We overviewed the technical detail and architecture of our system and illustrated the benefits it could provide; displaying high level, situational awareness to both cyber service providers and decision makers.

References

1 Musman, S., Temin, A., Tanner, M., Fox, D., and Pridemore, B.: 'Evaluating the Impact of Cyber Attacks on Missions', in Editor (Ed.)^(Eds.): 'Book Evaluating the Impact of Cyber Attacks on Missions' (The MITRE Corporation, 2009, edn.), pp.

2 Reith, M.L.C.: 'Forging Tomorrow's Air, Space and Cyber War Fighters', Air & Space Power Journal, 2016, Winter 2016

3 Maj Pritchett, M.: 'Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment', Air Force Institute of Technology, 2012

4 Lt Gen Bender, W., and Col Bryant, W.: 'Assuring the USAF Core Missions in the Information Age', Air & Space Power Journal, 2016

5 Defense, D.o.: 'Department of Defense Directive 3020.40. DoD Policy and Responsibilities for Critical Infrastructure', in Editor (Ed.)^(Eds.): 'Book Department of Defense Directive 3020.40. DoD Policy and Responsibilities for Critical Infrastructure' (2012, edn.), pp.

6 Force, U.S.A.: 'Air Force Doctrine Document 3-12. Cyberspace Operations', in Editor (Ed.)^(Eds.): 'Book Air Force Doctrine Document 3-12. Cyberspace Operations' (2010, edn.), pp.

7 Jabbour, K., and Muccio, S.: 'The Science of Mission Assurance', Journal of Strategic Security, 2011, 4, (2), pp. 61-74

8 Abercrombire, R.K., Sheldon, F.T., and Grimaila, M.R.: 'A Systematic Comprehensive Computational Model for Stake Estimation in Mission Assurance - Applying Cyber Security Econometrics System (CSES) to Mission Assurance Analysis Protocol (MAAP)', 2010, pp. 1153-1158

9 Schulz, A.E., Kotson, M.C., and Zipkin, J.R.: 'Cyber Network Mission Dependencies', in Editor (Ed.)^(Eds.): 'Book Cyber Network Mission Dependencies' (Massachusetts Institute of Technology, 2015, edn.), pp.

10 Bodeau, D., Graubart, R., and Heinbockel, W.: 'Mapping the Cyber Terrain', in Editor (Ed.)^(Eds.): 'Book Mapping the Cyber Terrain' (MITRE, 2013, edn.), pp.

11 Bryant, W.C.: 'Mission Assurance through Integrated Cyber Defense', Air & Space Power Journal, 2016, Winter 2016

12 USSTRATCOM/J663: 'Mission Assurance Decision Support System (MADSS) Concept of Operations v2.01', in Editor (Ed.)^(Eds.): 'Book Mission Assurance Decision Support System (MADSS) Concept of Operations v2.01' (2014, edn.), pp.