Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Assessing Mission Performance for Technology Reliant Missions

Noah DeMoes
MIT Lincoln Laboratory
noah.demoes@ll.mit.edu

Trang Nguyen
MIT Lincoln Laboratory
trang.nguyen@ll.mit.edu

Jaime Peña
MIT Lincoln Laboratory
jdpena@ll.mit.edu

Neal Wagner
Systems & Technology Research
neal.f.wagner@gmail.com

Abstract

Operators today increasingly rely on technology to accomplish objectives. Although technology can increase mission success and efficiency in a majority of operations, it can simultaneously increase vulnerability prevalence, resulting in a higher exploitation likelihood. Defense methods have been proposed and evaluated based on their ability to ensure network security. However, these evaluation metrics do not fully quantify how network exploitation impacts mission task completion. Our mission performance model links cyber devices to mission tasks utilizing a missions mission map and evaluates a missions performance as the proportion of completed mission tasks in an agent based simulation. Our model allows for mission mappings with varying degrees of completion to enable a generic and adaptable model. We investigate the impact differing levels of mission map completion have on the mission performance metric for the same mission. Experiments serve to provide quantitative assessment for mission performance in cyber-network mission systems.

1. Introduction

The reliance on technology in todays operational environment lowers the barrier for adversaries to conduct cyber-attacks through network vulnerability exploitation. A cyber attack is an attack, via cyberspace, targeting an enterprises use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure [1]. In 2017 alone, the Internet Crime Complaint Center received a total of 301,580 cyber-attack complaints that resulted in over $1.4 billion in reported losses [2]. Several companies have created and published various methods to mitigate cyber attack impact that either prevent cyber-attacks from occurring or mitigate the effects of a cyber intrusion [3] [4] and [5]. However, a gap exists in the quantitative evaluation of mitigation technique effectiveness.

Mitigation technique effectiveness is a measure of a mitigation techniques ability to stop potential attacks, slow intrusion damage, prevent mission delay, or increase mission performance. Mission performance is the proportion of completed tasks to the total number of mission tasks. There are several metrics used to represent mitigation effectiveness, such as security index, mission delay, and maintenance cost. For example, Wagner introduces a risk score for mission effectiveness for network segmentation that combines security index, mission delay and maintenance cost [6]. Although the risk score provides insight into a defense mitigation techniques ability to reduce risk to the network, it does not identify which mission tasks are affected by a specific device being compromised. Metrics like risk score measure a networks ability to defend against cyber-attacks, but do not provide a measurement of the mitigation techniques ability to enable mission objective completion. Without metrics that incorporate mission mappings to evaluate and rank each mitigation tool based on mission task completion, practitioners default to expert knowledge or personal experience to determine method implementation. Mission mapping is the process of identifying and linking each mission tasks cyber dependencies, the network topology, and the probability of compromise (POC) for each cyber asset. Additionally, network security is not the end state for most practitioners, but a means to accomplish mission objectives. Thus, mitigation technique effectiveness is synonymous with mission performance. Mission accomplishment relies on users, devices, and services working in tandem to accomplish all tasks users are assigned. Accordingly, any metric measuring mitigation effectiveness should consider the accomplishment of mission objectives in the context of the entire mission map as part of mission performance.

It is important to note that a cyber mission map contains users, devices, services, and mission tasks as well as probabilities of compromise (POC) for each

URI: https://hdl.handle.net/10125/63920
978-0-9981331-3-3

device, user and service [7]. In this paper, when referencing users, devices and services together the word mission entities will be used. In the presence of the same mission map, mission entities will be compromised based on their POC. Thus, numerous tests are required to compute the expected outcome for mission performance for a given cyber mission map. Real-world implementation has high financial and time costs.

In this work we propose a novel mission performance metric that incorporates a missions mission mapping to compute the expected proportion of completed mission tasks. This metric differs from current metrics by reducing the network entities used to evaluate mission performance to only mission entities. Utilizing only mission entities results in a more specific mission performance metric over current methods. Our mission performance model is an adaptable simulation model that enables varying mission mapping types. In this paper, we evaluate the results for differing levels of information for mission maps by comparing the mission performance output for different mission mappings of the same mission.

2. Related Work

2.1. Mission Mapping

A mission map is a directional dependency graph of mission assets and network assets that informs decision makers on how to optimize resource allocation and adjust network architecture to best achieve results by identifying Cyber Key Terrain (CKT). There have been several technologies developed to create mission mapping. Some are fully autonomous, while some remain fully manual. An exhaustive survey exists here [8]. Schulz found that no technology exists that is fully automated while fully manual methods of mission mapping are effective and focus should be spent on mapping network capabilities.

Jeffery Guion focuses on creating a mission mapping that is mission oriented and not IT focused. Guion provides a framework on how to approach the problem and a dynamic mission mapping solution, but does not identify the features required to identify CKT [9].

Cyber Assets to Mission and Users (CAMUS) was created to map assets to mission devices with decent performance. It requires a large database of data in order to gather relationships, but does not include relationship metrics [10]. A study of using density of communications and common neighbors to identify mission devices on a network is presented in [11]. Mission mapping is a problem that has, yet to be fully solved. Current solutions yield mission maps that are either too static to be effective and distributable, or too generic to draw significant conclusions [12]. While this research focuses on mission mapping, it does not evaluates the ability to mission mapping nor the impact a mission map has on informing mission performance. In this paper we take a full, semi, or no mission map and evaluate the mission performance given the current mission map.

2.2. Mission Impact Metrics

A study that evaluates segmentation architecture utilizing a continuous Markov chain to model changes in network states is provided in [7]. A modularized hierarchical simulation framework to model a complete cyber system and evaluate the effectiveness of network-level mitigation techniques using security and mission impact metrics is demonstrated in [13]. An agent-based simulation is created to find the optimal network segmentation based on mission delay and security is found in [14]. A hybrid approach using nature-inspired optimization and cyber risk modeling and simulation created candidate network architectures based on security, cost, and mission performance metrics is found in [6].

Although applicable for network segmentation, the metrics found in these papers do not extend to other mitigations. In this paper we provide a mission performance metric that is agnostic to a mitigation techniques, making it adaptable and generic. Additionally, current methods measure mission impact as a function of the entire network. However, missions exist in which an entire network is not necessary for mission accomplishment. In such cases, if network entities that are unrelated to a mission are unavailable, current mission impact metrics incorporate this unavailability into mission performance, lowering its score, even though these entities do not play a role in this mission. Our mission performance model determines which network entities are mission critical through a missions mission mapping and evaluates performance based only on mission dependent entities.

3. Modeling Mission Performance

A mission map is a directed graph in which a mission model is mapped to a network graph. A mission model is a directed graph that depicts the tasks and non-cyber mission entities needed for a mission. The resulting mission map contains the mission tasks and each tasks non-cyber and cyber mission entities. This graph contains the following mission entities: mission tasks, users, devices, resources, and services as

nodes. Examples of mission entities include: humans, computers, servers, data, and software. Edges represent dependencies and are weighted with a source nodes mission capacity, the maximum number of mission tasks a node can complete.

Additionally, we define both soft and hard constraints for mission mappings that are informed by specific mission objective requirements. A soft constraint is a mission requirement that when unsatisfied results in a failure for the task dependent on that specific requirement. Although, that mission task failed, the mission can continue or still be semi-completed. A mission hard constraint is a mission requirement that must be satisfied to complete any part of the mission. If a mission hard constraint is violated, the mission performance automatically becomes zero. Mission mapping provides a methodology to identify soft and hard mission constraints.

3.1. Mission Entities

A mission device is any hardware that is required to complete a mission. Mission users are entities that use mission. A mission service is any software service needed to complete a mission. A mission resource is information or items needed to complete a mission. Devices can also store resources that are accessed through connections in services. For example, the Air Forces Air Operations Center (AOC) gathers and processes flight plans for air missions. In this example, the mission devices are MAAP Server, ATO Server, and the mission user are computers. Additionally, a device has a compromise rate that is a result of cleansing rate, patch rate, vulnerability rate, and exploitation rate parameters [7]. We utilize the probability of compromise results from Wagner as the probability of compromise for devices [7].

A mission user is an individual tasked to complete the mission. Mission users are constrained by the training that they have fulfilled. Some mission users are specialists and can only accomplish specific mission while other mission users are general users that can perform variety of mission tasks. Mission user information is provided from the mission model because they are non-cyber assets. The probability of compromise for cyber assets represents the likelihood that an asset is unavailable. Similarly, mission users become unavailable when absent from their job. Military members are afforded 2.5 days of leave per month. The probability that a member is absent from work on a given day is 0.0833, the number of leave days divided by 30. For the purpose of uniformity we will define the probability of absence for a mission user as a mission users probability of compromise. Mission users are connected to mission tasks through mission devices and services. Mission user capacity is a measure of the number of mission tasks a user is able to perform within the duration of the mission.

A resource is a packet of information needed to complete the mission. Air traffic orders are an example of a resource in the AOC example. Resources are connected to tasks through connections to devices and services. We assume that resources can be accessed at any time and that they are readily available. Based on this assumption resources do not have a capacity. Resources are assumed to be compromised if the device they are located in is compromised.

A services is software used to communicate between hardware. Some mission tasks require specific software. Other times, multiple software packages can accomplish the task. For example, if a mission task is to send a document between individuals, users could use email, deposit it on a shared server, or upload to the cloud. Services connect to tasks based on the software needed to complete the mission. The probability of compromise of a services is taken from [7].

A mission task is the final mission entity and is a job that is to be completed to meet mission objectives that requires a combination of users, devices, resources and services. Some mission tasks are dependent on other mission tasks. For example, in order for an air traffic order to be issued a master air attack plan must be completed.

3.2. Mapping Mission Entities

Traditionally mission mappings are created only when the complete mapping is known. If a full mission mapping with complete network structure is provided, connections are formed based on its depiction. However, this information is rarely available in an appropriate time frame. To mitigate this cost we propose a method to create partial mission mapping. When partial information is known about the mission map, the remaining information is approximated using probability distributions and Monte Carlo simulation. For example, the POC for each of the mission entities is unknown. To determine these probabilities users can search for average exploitation rates for hardware and software to approximate for the POC for devices and services, respectively. If a semi-full mission mapping is provided the full mission mapping must be created by connecting mission entities to mission tasks based on probabilities of connection and utilizing simulation.

Traditionally, mission mapping is represented by dependency graphs as displayed in Figure 1. The

independent mission entities are on the bottom level and subsequent levels represent the next entity that is dependent until the mission is achieved. This depiction is beneficial for visually identifying dependent entities for in small mission mappings, but makes it more costly to identify when mission tasks fail. In the case of large mission mappings the advantage of visual representation is diminished and mission task failure identification remains challenging.

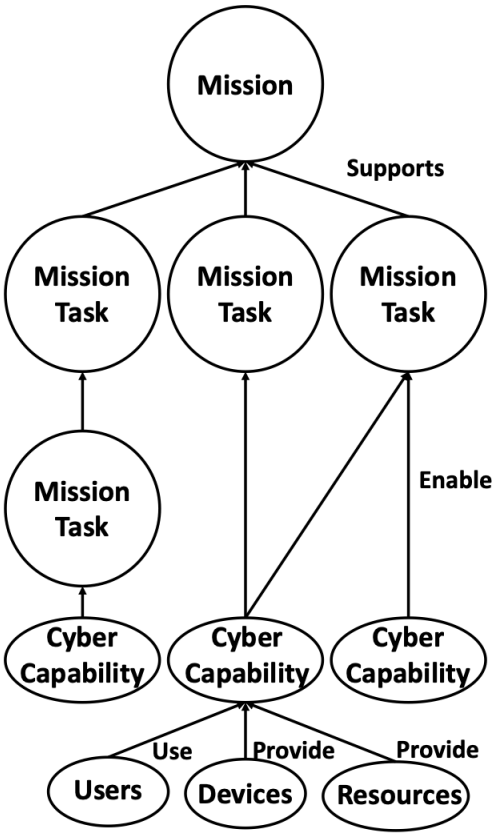

Figure 1. A traditional mission map.

To mitigate this disadvantage, we created a different mission map representation. We define a mission task i, as failed when any dependent mission entity for mission task i are compromised or unreachable. To quickly identify when a mission task fails, we map mission entities to mission tasks only. Thus, we simply look at the entities attached to a given mission task to see if they have been compromised. If they have, then we know that that mission task cannot be complete. The benefit is a more efficient method to determine connectivity with respect to mission tasks. Figure 2 provides an example of the new style of a mission map.

3.3. Mission Performance Metric

In addition to connectivity, each mission entity has both soft and hard constraint characteristics. The constraints are defined by the mission requirements. Soft constraints represent uniformity and adaptability for a given entity. For example, a soft constraint for devices is that at least one device must be used to complete mission task 1. The device need to complete the mission is left unspecified which increases the flexibility of the task. In contrast, a hard constraint represents a constraint that must be satisfied in order for the mission to be completed. For example, user 1 must be used to complete mission task 4 to accomplish the mission is a hard constraint because if user 1 cannot complete mission task 4 then the mission fails.

The final score for mission performance is the minimum between soft constraint mission performance ($SCMP$) and hard constraint mission performance ($HCMP$). If any hard constraint is violated, $HCMP$ receives a score of 0 and mission performance is 0. This makes sense because hard constraints represent requirements that must be completed to perform the mission. If one of those requirements is not fulfilled then the mission does not run. On the other hand, if no hard constraints are violated, then $HCMP$ is one and the minimum between $HCMP$ and $SCMP$ is $SCMP$.

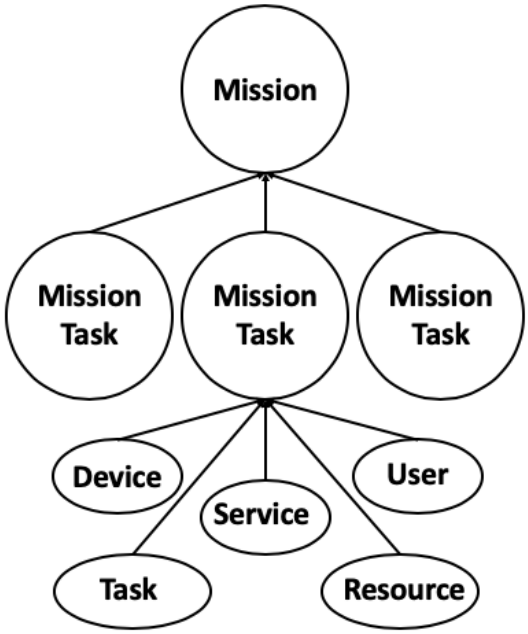

Figure 2. Our adaptive mission map.

Soft constraint mission task performance ($SCMTP$) measures the mission performance

given that no hard constraints were violated. Table 2 displays categories that influence mission performance and their corresponding soft constraints. The categories are time, order, adaptability, accessibility, and usability. These categories were selected because each one defines the availability of a mission entities. Time and order measure a tasks ability to be accomplished. Adaptability measures the availability of services. Accessibility measures the availability of resources. Usability measures the availability of users and devices because users are attached to devices to connect to the network. $SCMTP$ is calculated for task i:

$$SCMTP(t_i) = min\{T(t_i), O(t_i), A(t_i), AC(t_i), U(t_i), \}$$

where $T(t\_i)$ is the time score, $O(t_i)$ is the order score, $A(t_i)$ is the adaptability score, $AC(t_i)$ is the accessibility score and $U(t_i)$ is the usability score for soft constraints for task i. Each score is either 0 if the soft constraint is violated or 1 if the soft constraint is not violated. Thus, $SCMTP(t_i)$ is only 1 or 0. The $SCMP$ for the entire mission is:

$$SCMP = \frac{\sum_{i=1}^{n} SCTMP(t_i)}{n}$$

which is a value between 0 and 1.

Table 1. Mission performance hard constraints.

Category	Hard Constraint
Time T(t_i)	If the total time to complete all tasks exceeds the total mission time constraint, HCE=0. If the time score for a mission essential task is 0, HCE=0; else HCE=1.
Order O(t_i)	If there exists a mission essential task that is dependent and its order score is 0; HCO=0; else HCO=1.
Adaptability A(t_i)	If the availability score of a mission essential task is 0, HCA=0; else HCA=1.
Accessibility AC(t_i)	If the accessibility score of a mission essential task is 0, HCAC=0; else HCAC=1.
Usability U(t_i)	If the usability score of a mission essential task is 0; HCU=0; else HCU=1.

Hard Constraint mission performance ($HCMP$) measures whether or not the mission fails by identifying which mission entities violate any hard constraints. Table 1 provides a summary of the mission performance hard constraints. Categories are selected based on the same methodology as the soft constraint methodology. $HCMTP$ is calculated for task i:

$$HCMTP(t_i) = min\{T(t_i), O(t_i), A(t_i), AC(t_i), U(t_i)\},$$

where $T(t_i)$ is the time score, $O(t_i)$ is the order score, $A(t_i)$ is the adaptability score, $AC(t_i)$ is the accessibility score and $U(t_i)$ is the usability score for hard constraints for task i. If any $HCMTP$ is 0, the $HCMP$ is 0, else $HCMP$ is 1. Table 1 provides a summary of the mission performance hard constraints.

Table 2. Mission performance soft constraints.

Category	Soft Constraint Level 1	Soft Constraint Level 2
Time T(t_i)	Unrestricted time tasks receive time score of 1.	Time tasks that exceed constraint receive time score of 0.
Order O(t_i)	Independent tasks receive an order score of 1.	Dependent tasks receive an order score of 1 if all their dependent tasks have an order score of 1. Else score of 0.
Adaptability A(t_i)	If at least one service is available and connected to a task, score of 1. Else score of 0.	If the one service is available and connected to the task, score of 1. Else score of 0.
Accessibility AC(t_i)	If there exists a path between the task and resources needed for the task, accessibility score of 1. Else score of 0.	If there exists a path between the task and resources needed for the task, accessibility score of 1. Else score of 0.
Usability U(t_i)	If at least one user is connected to a mission task, usability score of 1; else usability score of 0.	If at least one user capable of completing the task is connected to the task, usability score of 1 else usability score of 0.

Thus, mission performance is the minimum between $SCMP$ and $HCMP$.

3.4. Mission Simulation

It is too costly to compute mission performance using test beds. An event-based mission simulation was chosen instead to mitigate cost. The objective of the simulation is to compute the expected value for mission performance, given a full or semi defined mission map.

For our model a simulation run is defined as follows: (1) instantiate all mission model entities (devices, users,

resources, services, and tasks and mission topology) and define all state variables, (2) generate events based on probability of compromise associated with each mission entity, (3) run until steady state is reached for the expected mission performance of each mission task, and (4) average mission performance across all mission tasks to get the expected mission performance for a given mission.

In addition to mission performance, the mission performance for each individual mission task is reported. This information is critical for risk assessment in the following ways: (1) understanding the mission task that is most likely to fail can provide insight on whether the mission should still be attempted, i.e. that mission task is unimportant and (2) identifying the mission entities that failed can help determine where network resiliency techniques should be prioritized to optimize benefit and reduce cost.

4. Experiments

The simulation utilized in this experiment is designed to model how cyber system entity behavior influences completion likelihood for mission tasks in order to provide a metric that measures the impact mitigation tools have on mission performance. The mission performance model is implemented in NetLogo [15]. A comparison between mission performance among a fully defined, semi defined and ill-defined mission map for an AOC mission is conducted to demonstrate the models adaptability. It is far more likely, that a semi-defined or low-defined mission map is available because techniques to mission map are still not complete. Additionally, the time associated with creating a full mission map often is too costly with respect to mission duration. Comparing semi defined and ill-defined mission map mission performance to fully defined performance provides insight into the accuracy of the metric, and in which instances it is acceptable to only create semi defined or ill-defined mission maps as opposed to a full mission map.

4.1. Full mission map experimental setup

The AOC mission used in our experiment contains three mission tasks, three mission users, three resources, three mission devices, and three services. A full mission map would provide how each of these entities are specifically connected and the probability of compromise associated with each network device. A complete AOC mission map does not exist, but we created a predicted full mission model to demonstrate the mission performance models ability to handle full mission maps. For this mission map we connect mission user 1, device 1, service 1, and resource 1 to mission task 1. This connection methodology is the same for the other two mission users because that is what is depicted in the AOC mission map and is depicted in Figure 3. Additionally, there are dependent tasks. Task 1 is dependent on Task 0 and Task 2 is dependent on Task 1. The probability of compromise for users is 0.0833 based on the number of leave days each soldier has. For both services and devices the probability of compromise is 0.10 and is derived from [13]. It is the average POC from a variety of exploitation, and patch rates with cleaning rate of 25 days. Exploitation rate is the rate at which an adversary creates and deploys an exploit. Patch rate is the rate at which exploitations are discovered and patched. Cleansing rate is the rate at which the devices and soft wares are updated and cleaned. The time constraint for each task is 1 day, and 3 days for the entire mission. Simulation time is defined such that 1,000 time units = 1 day. Results are collected from 1,500 Monte Carlo simulation runs that are terminated after 3,000 time simulation time units.

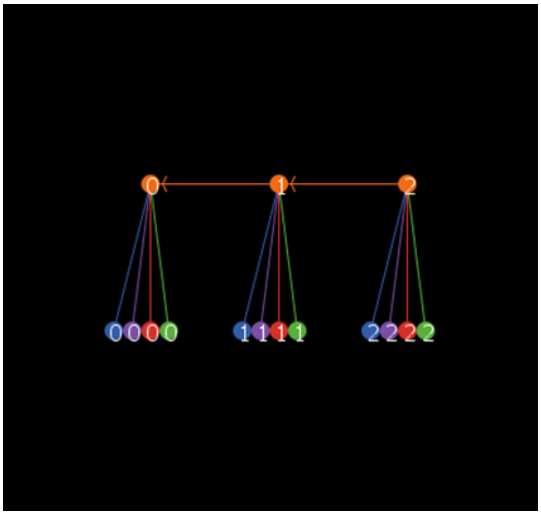

Figure 3. A full AOC mission map.

As seen in Figure 3, the mission tasks are represented in orange, the services in red, devices in green, resources in violet, and users in blue. Task 1 is dependent on Task 0 and Task 2 is dependent on Task 1. Unlike semi-defined and ill defined mission maps, the only factor that impacts connectivity is the probability of compromise. If the probability of compromise is zero for a complete mission map, then the map will never change because the map is fully supplyed by the customer.

4.2. Semi-defined Mission Map Setup

A semi-defined mission map is a map that has some elements missing. To mitigate this issue values are selected from probability distributions to replace them. The missing elements could represent anything from unknown values for the probability of compromise to missing device connections to the network. In either instance, we assign the missing value with an expected value based on prior knowledge. For this AOC semi-defined mission map used in our experiment, the number of entities is the same as the full mission map, however we define connectivity as unknown. To mitigate this, we define a probability of connectivity of 0.60 and define POC as 0.08333. We chose probability of connectivity to be 0.60 because it is likely that most military mission entities are set up in the same way and thus each entity is fairly likely to be connected to another. For example, if a mission map does not provide the connections between mission entities, the model provides a probability of connection that assigns entities to entities based on that probability. Once assignment occurs, the mission performance is calculated for 1,500 Monte Carlo simulation runs.

4.3. Undefined mission map

An undefined mission map is a mission map that provides the bare minimum of information to run a simulation. For example, in our model the only information known is the mission tasks, mission users, and the mission constraints. In this instance, the probability of compromise, probability of connectivity, and the network must be approximated. The probabilities for both are drawn from uniform distribution between 0 and 1. This distribution was only selected for demonstration purposes. It should be noted that in an undefined mission map the probability distribution can be anything with distribution between 0 and 1. A better method may be to estimate the distribution of available network data with a kernel density function that best approximates the distribution and create connections from that distribution. The outcome for mission performance is significantly tied to the probabilities selected.

5. Results

Table 3 displays the mission performance results and probabilities of compromise for each mission entity for each of the three mission mapping types. Figures 4 and 5 provide experimental results for the AOC mission. Figure 4 show mission performance results for each task and for each of the three mission mapping types tested. Figure 5 shows the expected mission performance for the AOC mission for each of the three mission mapping types.

Table 3. Mission map characteristics and their resulting mission performance..

Mission Map	Full	Semi	Undefined
User POC	0.0833	0.0833	0.0833
Device POC	0.1	0.1	[0, 0.5]
Service POC	0.10	0.10	[0, 0.5]
Resource POC	0.10	0.10	[0, 0.5]
Connections	Known	0.60	[0,1]
Mission Performance	0.5126	0.5126	0.2826

As seen in Table 3, the full mission map is completely known with mission performance score of 0.5126. The semi-defined mission map has POCs defined for each mission entity, but the network map is unknown. For this experiment we assumed a probability of connection for each mission entity to be 0.60. In practice, this value will be selected based on expert knowledge or approximation from other similar mission mappings. Again, for any semi-defined map any of the categories in Table 3, such as Service POC could be missing, which would require an approximation. Because of the high cost associated with false negatives, we selected a probability of connections that is low to produce more conservative results. The undefined mission map has only one constant value for user POC because their availability is independent of the cyber network. Everything is unknown which requires a value to be selected for each POC for each iteration for each mission entity. Figure 4 below shows the difference in results for each mission task and each mission mapping.

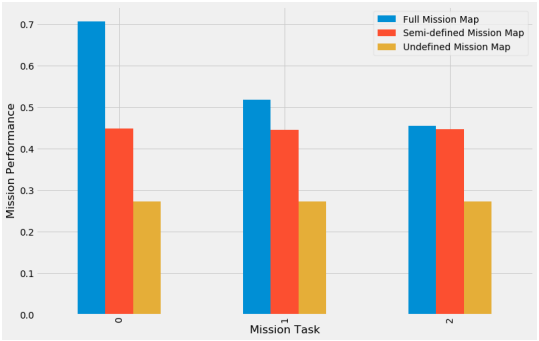

Figure 4. Mission performance by mission map type and by task.

In Figure 4 we give mission performance results for each of the mission tasks as the expected probability that the mission task will be completed for three different mission maps. It is apparent that mission Task 0 had the greatest variance among its three mission maps as compared to mission Task 1 and mission Task 2. This could be due to the task dependencies in the full mission map which would result in lower mission performances for Task 1 and Task 2 because they fail every time when Task 0 fails and when themselves fail.

Additionally, as the level of information a mission provided decreased, the expected mission performance also decreased. This is more due to the conservative values we selected for the values we had to select for the missing information in the semi defined and ill-defined mappings. We could have set the missing POC values to 1 and get great mission performance, but that is not the intent of the metric. The metric is designed to provide practitioners with mission centric results. For missions with low cost, it may be advantageous to be less conservative in approximating missing values because of the low risk. We also see that mission Task 2 failed more often than mission Task 0 and Task 1. This can be explained by the dependency Task 2 has on Task 1 and Task 0.

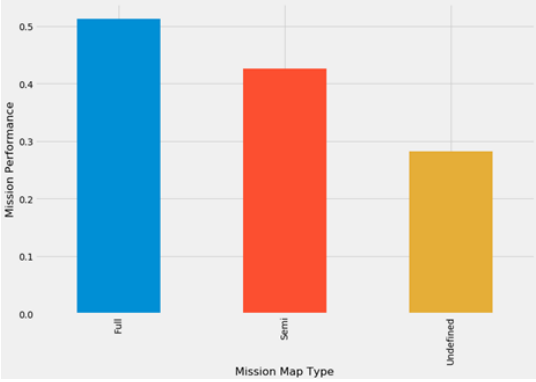

Figure 5. Expected mission performance by mission map type.

Figure 5 shows the average mission performance among the three mission tasks for each mission mapping. For these experiments, Figure 5 shows that the more information the mission map contains, the higher expected mission performance. Overall, there are three key observations from the experimental results. First, the mission performance metric produces logical results. Semi and undefined mission maps contain more assumptions about the network. We used larger values for probability of compromise because of the high cost of false negatives which would result in lower mission performance as shown in Figure 5. Second, although complete mission mapping remains a complex, dynamic problem, utilizing a semi mission map and our mission performance metric may provide satisfactory results for some missions. Third, the mission performance is approximately 50% which may be unlikely. As a means to inform the POCs for incomplete mappings, a customer may use prior mission performance to better approximate POCs.

6. Conclusion

In this paper, we discussed mission mapping and challenges that exist in mapping missions to network topologies such as time and money. We also illustrated that as a result of these challenges there is not a generic and adaptable metric to measure mission performance. We developed a novel mission performance metric that can produce a mission performance for mission maps that enables flexibility in in the level of information provided by the input. Our metric also provides greater specificity and granularity in evaluating mission performance than current methods by representing mission performance as a function of mission critical network entities instead of as a function of the entire network. In addition to providing a performance metric for the entire mission, our model enables evaluation at the mission entity level to provide the user information on where to focus resources. This metric can be viewed by users as the expected probability that a mission will complete. The model is low-cost in both time and money and provides a quantifiable metric for practitioners to use in evaluating the defense mitigation effectiveness and mission resiliency.

Future work is focused on incorporating this mission performance model into cyber defense evaluation models to better evaluate cyber defense techniques in the context of the missions they support.

References

[1] J. T. Force and T. Initiative, "Security and privacy controls for federal information systems and organizations," *NIST Special Publication*, vol. 800, no. 53, pp. 8–13, 2013.

[2] S. Smith, "2017 Internet Crime Report ," tech. rep., Federal Bureau of Investigation, 2018.

[3] Google, "Googles Approach to IT Security," tech. rep., Google, 2012.

[4] Microsoft, "Enterprise Security Best Practices ," tech. rep., Microsoft, 2015.

[5] NSA, "NSAs Top Ten Cybersecurity Mitigation Strategies ," tech. rep., National Security Agency, 2018.

[6] N. Wagner, C. Ş. Şahin, J. Pena, and W. W. Streilein, "Automatic generation of cyber architectures optimized for security, cost, and mission performance: A nature-inspired approach," in *Advances in*

Nature-Inspired Computing and Applications, pp. 1–25, Springer, 2019.

[7] N. Wagner, C. Ş. Şahin, J. Pena, J. Riordan, and S. Neumayer, "Capturing the security effects of network segmentation via a continuous-time markov chain model," in *Proceedings of the 50th Annual Simulation Symposium*, p. 17, Society for Computer Simulation International, 2017.

[8] A. E. Schulz, M. C. Kotson, and J. R. Zipkin, "Cyber network mission dependencies," tech. rep., MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB, 2015.

[9] J. Guion and M. Reith, "Dynamic cyber mission mapping," in *IIE Annual Conference. Proceedings*, pp. 1925–1931, Institute of Industrial and Systems Engineers (IISE), 2017.

[10] J. R. Goodall, A. D'Amico, and J. K. Kopylec, "Camus: automatically mapping cyber assets to missions and users," in *MILCOM 2009-2009 IEEE Military Communications Conference*, pp. 1–7, IEEE, 2009.

[11] J. Pattillo, "Mission mapping," tech. rep., MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB, 2011.

[12] A. Schulz, M. Kotson, C. Meiners, T. Meunier, D. OGwynn, P. Trepagnier, and D. Weller-Fahy, "Active dependency mapping," in *International Conference on Information Reuse and Integration*, pp. 169–188, Springer, 2017.

[13] N. Wagner, C. Ş. Şahin, M. Winterrose, J. Riordan, D. Hanson, J. Peña, and W. W. Streilein, "Quantifying the mission impact of network-level cyber defensive mitigations," *The Journal of Defense Modeling and Simulation*, vol. 14, no. 3, pp. 201–216, 2017.

[14] N. Wagner, C. Ş. Şahin, M. Winterrose, J. Riordan, J. Pena, D. Hanson, and W. W. Streilein, "Towards automated cyber decision support: A case study on network segmentation for security," in *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1–10, IEEE, 2016.

[15] U. Wilensky, "Netlogo," http://ccl.northwestern.edu/netlogo/, Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL, 1999.