Building Mission-Centric Cyber Risk Assessments

Jeffrey Guion, Mark Reith
Air Force Institute of Technology, Wright-Patterson AFB, OH
jeffrey.guion@afit.edu
mark.reith@afit.edu

Abstract: Risk assessments are a standard practice within the Department of Defense (DoD) operation planning process. However, many operational missions do not adequately incorporate dependence on cyberspace into their risk management cycle. In today's contested cyber environment, not considering how vulnerabilities and threats to information systems and networks may impact a mission's execution can result in essential data being stolen, modified or unavailable causing mission degradation or failure. The DoD Information Network Risk Assessment Methodology (DoDIN-RAM) is a framework for assessing risks to DoD mission functions enabled by cyberspace. This method was created by United States Cyber Command and incorporates guidelines from National Institute of Standards and Technology (NIST). DoDIN-RAM considers four primary factors in making a qualitative risk assessment: threat, vulnerability, likelihood and mission impact. This paper applies the DoDIN-RAM to our cyber terrain mission mapping tool then proposes and demonstrates a model for building mission specific cyber risk assessments. We have previously demonstrated the importance of using cyber terrain mission mapping to capture the criticality of cyber assets towards successful completion of a mission. This allows us to calculate mission impact for each cyber asset. We expand our mission mapping framework to include a risk assessment capability based on the identified mission impact.

1. Introduction

Risk assessments are an important part of operational planning within the military. Mission planners will develop courses of action (COAs) and select the best COA based on minimizing risk and maximizing chance of success. The determination of which COA to choose often is based on operational art. Operational art is built on the commander and mission planner's experience, knowledge and intuition. For example, a commander of an Air Operations Center (AOC) will usually be a pilot with expertise in executing flying missions.

In today's information era, all military missions have a dependence on cyberspace for mission planning, scheduling, communication, intelligence gathering and many other functions. Military weapon systems are becoming more technologically advanced and having increasingly high dependence on cyberspace. The F-35, for example, has millions of lines of code. However, outside of cyber-specific career fields, mission planners have little experience and knowledge of vulnerabilities that can exist in cyberspace. This being the case, mission planners do not adequately consider cyber risk in the operational design process.

Cyber threat has been named the top strategic threat, according to Director of National Intelligence, since 2013. (U.S. Department of Defense, 2015) Military operations and weapon systems can be targeted covertly and near anonymously by adversaries. Information system users expect their cyber security service provider to protect all cyber terrain all the time. However, this is often infeasible due to cost and scope of cyber defense. Additionally, service providers typically do not have much interaction with the operators using information systems to execute a mission, so they do not know what systems are most important. In previous works, we outlined why cyber terrain mission mapping is a key component in providing mission assurance.(Guion and Reith, 2017b) In this paper, we present a risk assessment framework that uses mission mapping as an input for mission-based cyber risk assessments. We then demonstrate how this can be applied to create a semi-automated risk assessment tool.

2. Background

2.1 Mission Mapping

Mission mapping is the decomposition of a mission into key tasks that are required to execute the mission, and the identification of cyber dependencies supporting that task.(Guion and Reith, 2017a) This will typically form a tree or graph structure where the parent is a higher-level function or object and the children are nodes that support the parent. Each child can be given a criticality identifying its importance to the parent. This is used to identify which systems are the most important in accomplishing a mission and what the mission impact is if one of the cyber dependencies is unavailable or compromised. Mission impact assessments are reactionary, in response to some form of cyber threat. Risk assessments can be done preemptively to identify areas of higher risk to a mission based on those relationships identified during mission mapping.

Figure 1 is a simple mission mapping example. If an event occurs that impacts System One, because it has a high impact on Task One, the status of Task One and the overall Mission will be significantly degraded. On the other side, if an event occurs that impacts System Four, since it has a low impact on Task Two, the status of Task Two is only slightly degraded and workarounds are available to complete the task.

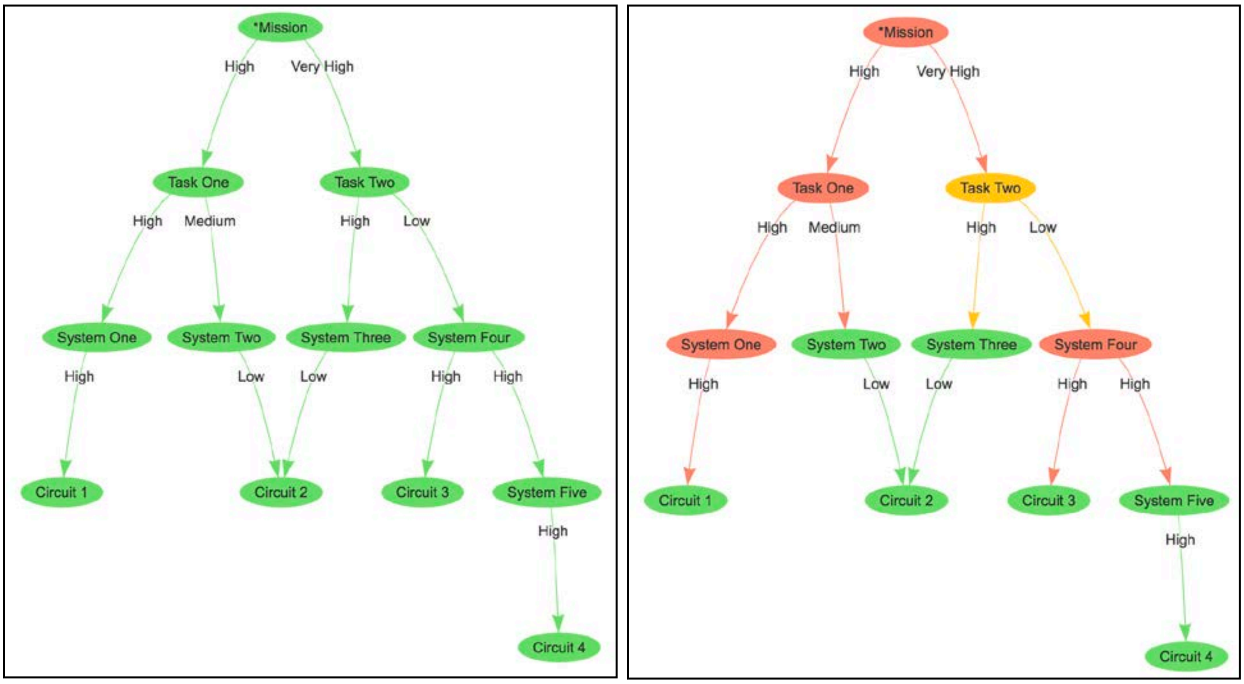


Figure 1. Mission mapping example

A similar framework can be used while calculating risk. If a system that is critical to execute a task has high risk of being compromised or taken down, then the risk to that task being accomplished is also high. However, if a system is not important for a mission, then the risk to that mission being accomplished is also low, even if the risk to that system is high. The next section will look into how to define risk to missions and risk to systems.

2.2 Risk Assessments

National Institute of Standards and Technology (NIST) develops many of the standards when it comes to assessing risk to information systems. NIST is the primary body for creating these standards for the Department of Defense (DoD). Following the NIST guidelines for risk assessment, United States Cyber Command (USCYBERCOM) along with supporting services and industry partners developed the DoD Information Network Risk Assessment Methodology (DoDIN-RAM). DoDIN-RAM is a framework for assessing risks to DoD mission functions enabled by cyberspace; it considers four factors in making a risk determination: vulnerabilities, threat, likelihood and impact. (U.S. Cyber Command, 2017) This methodology assigns each of the factors a qualitative value, between Very Low and Very High based on lookup matrices. We’ve included the matrices in Appendix A for convenience.

USCYBERCOM defines a *threat* as “any circumstance or event with the potential to adversely impact mission operations, through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.”(U.S. Cyber Command, 2017) Threats are events caused by threat sources which indicate adversary intent and method targeted at the exploitation of a vulnerability. Threat sources may also be non-adversarial such as the accidental exploit of a vulnerability or a natural event. NIST lists out the general types of threat sources as “(i) hostile cyber or physical attacks; (ii) human errors of omission or commission; (iii) structural failures of organization-controlled resources; and (iv) natural and man-made disasters, accidents, and failures beyond the control of the organization.”(NIST, 2012)

Threat modeling is a common practice both within the DoD and the private sector. Cyber threat models typically consist of a progression of labels which denote the motivations, sophistication and capabilities of the threat source: script kiddies, hacktivists, terrorists, organized crime, nation states. (Mateski *et al.*, 2012) Figure 2 is an example of a Cyber Threat Taxonomy from the DSB Task Force Report on Resilient Military Systems and the Advanced Cyber Threat.(DoD Defense Science Board, 2013) This form of taxonomy may be useful as a threat model but does not generate specific threats. Specific threats are typically collected as a combination of open source intelligence sharing, monitoring of network and host based sensors and dedicated intelligence cells. Examples of open source intelligence are Threat Advisories published by United States Computer Emergency Readiness Team (US-CERT) or rules posted by Emerging Threats in response to different types of attacks. These advisories will often contain indicators of compromise which are signatures of the threat event. Within the DoD, the intelligence cell will make a determination on the severity level of each threat event.

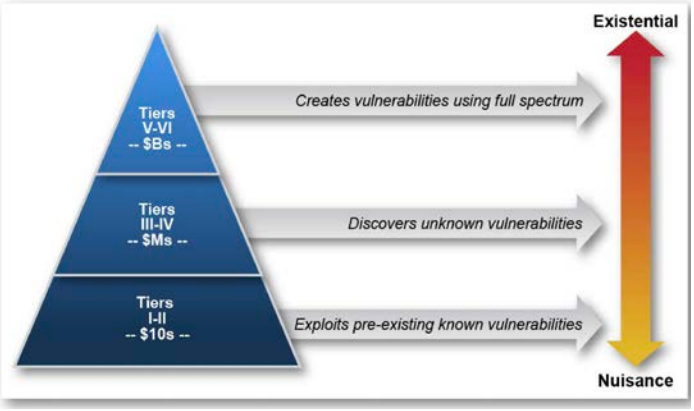

Existential
Tiers
V-VI
-- $Bs --
Creates vulnerabilities using full spectrum
Tiers
III-IV
-- $Ms --
Discovers unknown vulnerabilities
Tiers
I-II
-- $10s --
Exploits pre-existing known vulnerabilities
Nuisance

Figure 2. Cyber Threat Taxonomy(DoD Defense Science Board, 2013)

A *vulnerability* is a cybersecurity weakness that could be exploited by a threat source. It may be a known software vulnerability tracked in the National Vulnerability Database (NVD), or the failure to apply a security control. NVD includes quantitative scoring metrics such as severity, impact and exploitability as part of the Common Vulnerability Scoring System (CVSS). Exploitability, measured from 0.0 - 3.9, is a function of the attack vector, attack complexity, privileges required and user interaction in order to successfully exploit the vulnerability. Impact, measured from 0.0 - 6.0, is a function of the effect of the vulnerability to confidentiality, integrity and availability. The overall vulnerability severity, measured from 0.0 - 10.0, is a function of exploitability, scope, impact.(FIRST, 2017) Gathering vulnerabilities to a system is a combination of automated scanning using a vulnerability scanner and manual assessment.

Mission Impact is the degree of impairment to a commander's mission. In order to gather mission impact, an understanding of how a mission operates and the level of impact each information system has on a mission is critical. As outlined above, mission mapping is an effective way to make this determination.

Likelihood is the probability that a given threat is capable of exploiting a set of vulnerabilities. The likelihood factor is typically assessed as a weighted combination of adversary intent, adversary capability, the vulnerability exploitability and mission impact.(NIST, 2012) DoDIN-RAM scores likelihood as a function of threat and vulnerability.

Using these factors, we are able to create a qualitative or semi-quantitative risk assessments. Since some of the values are based on subjective judgment, typically performed by a subject matter expert, a qualitative risk assessment typically suffices with an acceptable degree of granularity for mission owners.

3. Methodology

Risk assessments have a defined risk model, assessment approach and analysis approach which are used to compute risk.(NIST, 2012) In this section, we will look at a couple variations of our model and assessment approaches. Our analysis approach is mission-oriented and assumes some form of cyber terrain mission mapping has been conducted and documented. Our risk model will consider the same risk factors, documented above, but the way to compute those factors and conduct the assessment will vary. Currently, most risk assessments are a one-time activity. For example, a mission owner will ask a Cyber Protection Team (CPT) to assess the risk to their mission based on its cyber dependencies. The CPT will perform the assessment and document a summary in a risk assessment report. This creates a static snapshot of a risk score to a mission or organization. With our proposed framework, we would like to create a more dynamic risk assessment which is automatically updated based on threats and vulnerabilities. The intent is to have a risk score you can look at for each execution of a mission rather than a one-time risk assessment. There are still required manual inputs and data sources that need to be synchronized but this is much less costly than starting new assessments from scratch. Additionally, it is important to be able to show exactly why a mission risk is what it is. Having a tool to show threats and vulnerabilities and how they are related and impact a mission will increase understanding for the mission owner.

Our goal was to create a framework that could be used by a DoD organization to assess the risk to their mission in a dynamic fashion. Rather than having to manually conduct a risk assessment, we use the relationships between mission impact, vulnerabilities and threats to automatically provide a risk score to a mission or task. This framework applies specifically to a mission mapping graph. As outlined in the mission mapping section, mission tasks as well as the systems that make up those tasks are nodes and the mission impact of that system is the edge between it and its parent. A mission impact is typically captured with a qualitative value ("Very Low", "Low", "Medium", "High" or "Very High").

3.1 Vulnerabilities

Vulnerabilities are typically applied at the system level. Known vulnerabilities with a CVE identifier are given a quantitative severity score by NVD which is a factor of the exploitability and impact of the vulnerability. These vulnerabilities can typically be identified through a vulnerability scanner such as Nessus. Other vulnerabilities can be identified on a system due to the lack of security controls. Typically, the security controls do not have their own quantitative score but may be given a qualitative rating from the importance of that control. Defense Information Systems Agency (DISA) publishes Secure Technical Implementation Guides (STIGs) which are configuration standards for DoD devices. Failure to comply results in CAT I, CAT II or CAT III vulnerabilities. Additionally, NIST Special Publication 800-53 lists recommended security controls for information systems and organizations.(NIST, 2013) Table 1 outlines vulnerability scoring to a qualitative rating for different types of vulnerabilities. Any additional vulnerability sources would similarly be given a manual score. Blue team or red team assessments are a good way to gather vulnerabilities that an attacker may try to target.

Our risk assessment model will take the maximum vulnerability severity and assign it as the vulnerability level for that system. This vulnerability score propagates upward based on dependencies and mission impact identified in mission mapping. The reason is it only takes one vulnerability to impact a system and therefore a mission. Our system is designed to track all vulnerabilities inputted though to provide a more detailed situational awareness picture for decision makers. We will use this formula to calculate maximum vulnerability severity:

$$\begin{aligned}&Vulnerability\ score = Max\ (Max\ (vulnerability\ severity\!: for\ each\ vulnerability),\\&\qquad f\,(dependency\ vulnerability\ score,\ dependency\ system\ impact)).\end{aligned}$$

Table 1. Vulnerability Scoring

NVD Vulnerability Severity	NIST Security Control Priority	DISA STIG Severity	Qualitative Vulnerability Score
9-10			Very High
6-9	P1	CAT I	High
4-6	P2	CAT II	Medium
2-4	P3	CAT III	Low
0-2	P0		Very Low

3.2 Threats

Threats are more difficult to measure. Threat assessments may be conducted to create threat source profiles which identify tactics, techniques and procedures (TTPs) of known threat actors which may have intention of targeting a system within your organization. Then the TTPs can be associated with targeted vulnerabilities or lack of security controls they exploit. The combination of threat and vulnerability is then manually assessed and given a qualitative likelihood and impact score. Table 1 is an example of a threat assessment using this methodology. Air Force Cyber Protection Teams often use this technique for conducting risk assessments. This analysis of threats requires intelligence sources to build a cyber threat assessment on known threat sources. This method works for measuring risk from persistent threats but doesn't provide a dynamic or automated risk assessment based on current threats campaigns and vulnerabilities.

Table 2. Sample Threat Assessment

Threat Source	TTPs	Vulnerabilities	Likelihood *(manual score)*	Impact (*manual score)*
APT1	Data Exfiltration	No Data Loss Prevention (DLP)		
		Insufficient network security devices		
		Insecure protocols		
	Insider threat	No DLP		
		Physical security		
		No two factor authentication		
Criminal Group	Malware injection	Out of date patching		
		Obsolete operating systems		
APT2	Spear phishing	Weak passwords		
		No security certificates		
	Denial of Service	Public facing web servers		
		Firewall rules		

Automated and dynamic threat information can be compiled from many different sources. US Government and Intelligence Community publish both classified and unclassified threat reports, vendors may publish threats targeting their products and private companies may provide threat intelligence as a service. Additionally, open source research of active threats and indicators may yield many results. US-CERT for example, will publish public Threat Advisories warning of adversary campaigns and what vulnerabilities they are targeting. One common cyber threat intelligence format that fits well into a graph representation of mission-centric risk assessments is Structured Threat Information Expression (STIX). STIX was created by MITRE and is a way to share cyber threat intelligence in a consistent and machine-readable format.(Struse *et al.*, 2017) The STIX architecture, outline in Figure 3, well expresses the relationships between entities of a cyber kill chain. A threat actor conducts campaigns which targets certain vulnerabilities. The threat actor may also target certain identities (individuals, organizations or groups). The threat actor uses TTPs which target vulnerabilities or identities. Observed data leads to indicators which can be associated back to threat actors or TTPs. This architecture defines the relationship between threats and vulnerabilities. If an adversary campaign is targeting a vulnerability that is located on a system in your organization, then that threat has the capability and demonstrates intent to exploit that vulnerability.

Measuring threat then requires expert judgement to pull together threat information, correlate them with vulnerabilities and assign a threat score. Dedicated intel cells typically will score threats based danger posed. Where available, this is a very valuable source of information and can be ingested. For our automated tool, we will focus on threats actors or campaigns that target vulnerabilities found in a mission mapping graph. The information sources may still need to be entered manually or ingested from STIX format but can be automatically correlated to any inputted vulnerabilities. Threat campaigns are instances of a threat pursuing an intent. Since threat score takes into account capability and intent, we'll argue an adversary campaign displays both of those factors which results in a Very High threat score where a targeted vulnerability exists. If an adversary TTP can exploit a vulnerability found, then the adversary capability exists but intent must still be evaluated. Threat events may be determined based on sightings and indicators. These events, if they can be correlated back to a threat actor, show adversary intent but the capability must be assessed. In these cases, there likely needs to be some form of judgement to provide an actual threat score.

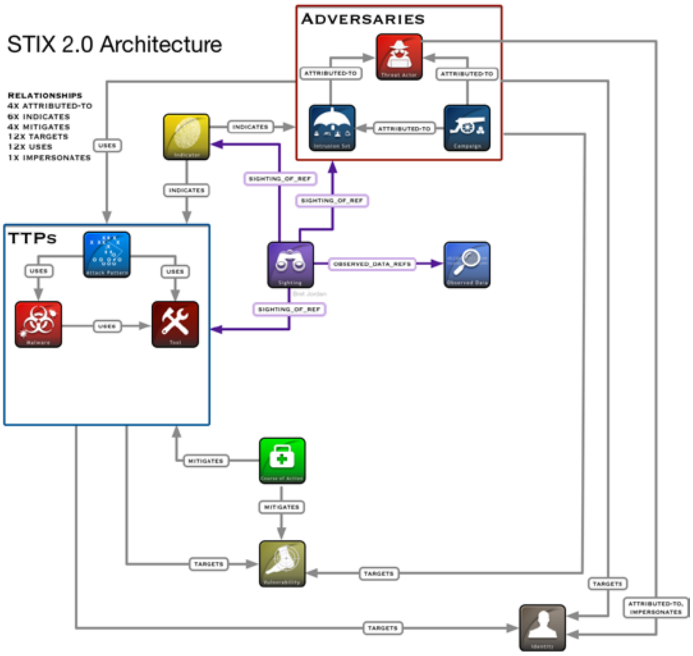


Figure 3. STIX Architecture (Struse *et al.*, 2017)

3.3 Likelihood

Likelihood may be its own factor or a combination of other factors which help produce the risk score. It is typically a qualitative probability that a threat can exploit a vulnerability and it will have an adverse impact. DoDIN-RAM scores likelihood as a function of threat and vulnerability. NIST does not define a likelihood function in a statistical sense but defines it as a score based on available evidence, experience and expert judgement.(NIST, 2012) For simplicity of applying the DoDIN-RAM, we will calculate likelihood as *Max(f(vulnerability, threat))* for each vulnerability and threat pairing. We will later offer some suggestions on how to account for the other factors. Since likelihood is measured at each system, we must also account for the likelihood an event occurs which impacts any dependent systems. For example, there is a high risk to a network router which provides connectivity to a system, there is also high risk that a system which relies on that network node cannot perform its necessary mission function without out. To account for this upward propagation, we will use this formula: *Likelihood = Max(f(vulnerability, threat), f(dependency likelihood, impact)).*

3.4 Mission Impact

Figure 4 demonstrates the relationships between threat, vulnerability and impact that allow us to calculate risk. Bringing it all together, we first calculate the likelihood an event happens at a system level, then propagate the risk up to the mission task based on *mission impact*. Mission impact is recorded during the mission mapping phase and each node identifies the importance of its dependencies. If a system has high likelihood of exploit but low impact to a mission, then the actual risk to that mission is low. While good cybersecurity practice dictates that vulnerability should still be addressed, it may be a lower priority than something that would have high mission impact. To calculate a risk score from a mission object, you take the highest risk to any dependencies based on their likelihood and mission impact to the given mission node. We use this risk formula:
Risk = Max(f(likelihood, mission impact): for each dependency).

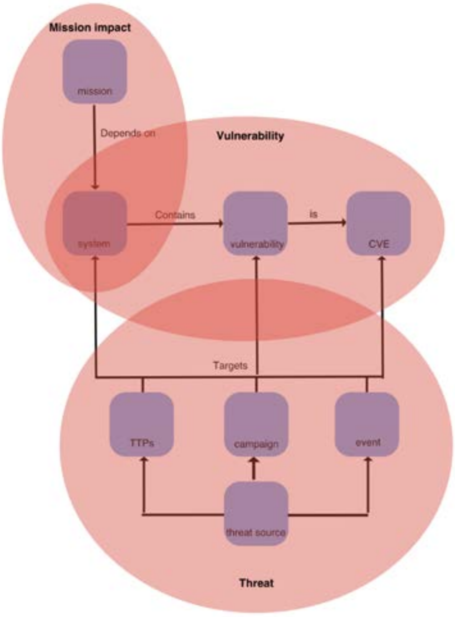


Figure 4. Risk factors

4. Results

In this section, we create a scenario and apply our risk assessment framework. We will use the small mission mapping example from Figure 1, threat information from Table 1 and Table 3 and vulnerabilities in Table 4.

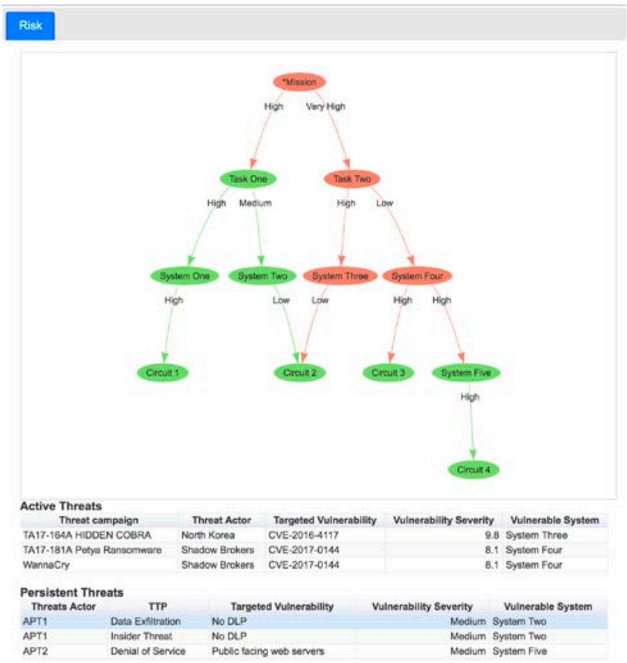
Table 3 Threats (US-CERT Threat Advisories)

Threat Actor	**Campaigns**	**Targeted Vulnerabilities**	**Severity / Exploitability**	**CIA Impact**
Shadow Brokers	Petya Ransomware TA17-181A	CVE-2017-0144 CVE-2017-0145	8.1/2.2	C:H; I:H; A:H
Lazarus Group	WannaCry TA17-132A	CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147	8.1/2.2	C:H; I:H; A:H
Lazarus Group	HIDDEN COBRA TA17-164A	CVE-2016-4117 CVE-2016-1019 CVE-2016-0034	9.8/3.9 9.8/3.9 8.8/2.8	C:H; I:H; A:H C:H; I:H; A:H C:H; I:H; A:H

Table 4 System Vulnerabilities

System	**Vulnerabilities**	**Score**	**Threat**	**Threat Level**	**Likelihood** *f(threat, vuln)*
System One	N/A	VL	N/A	VL	VL
System Two	No DLP	M	AP1	L	L
System Three	CVE-2016-4117	VH	HIDDEN COBRA	VH	H
System Four	CVE-2017-0144	VH	Peyta Ransomware WannaCry	VH	H
System Five	Public facing web server	M	APT2	M	M

Based on systems and vulnerabilities, we correlate threats to them in Table 4. Since HIDDEN COBRA, WannaCry and Peyta Ransomware were campaigns, their threat level is Very High. The threat from APT1 has been assessed as Low and the threat from APT2 has been assessed as Medium. Based on the vulnerability score and threat score, we use the look-up function from DoDIN-RAM (Appendix A) to produce the likelihood score. This likelihood score represents the probability an attack may occur which can impact a system. We then perform the mission impact calculation based on our mission mapping.



Active Threats

Threat campaign	Threat Actor	Targeted Vulnerability	Vulnerability Severity	Vulnerable System
TA17-164A HIDDEN COBRA	North Korea	CVE-2016-4117	9.8	System Three
TA17-181A Petya Ransomware	Shadow Brokers	CVE-2017-0144	8.1	System Four
WannaCry	Shadow Brokers	CVE-2017-0144	8.1	System Four

Persistent Threats

Threats Actor	TTP	Targeted Vulnerability	Vulnerability Severity	Vulnerable System
APT1	Data Exfiltration	No DLP	Medium	System Two
APT1	Insider Threat	No DLP	Medium	System Two
APT2	Denial of Service	Public facing web servers	Medium	System Five

Figure 5. Risk Graph

$$\begin{aligned}
&\text{Task one risk} = \\
&\quad \text{Max}(\, f(\text{Sys1 Likelihood, Sys1 Impact}), \\
&\qquad f(\text{Sys2 Likelihood, Sys2 Impact})) \\
&= \text{Max}\ (\, f(\text{VL, H}),\ f(\text{L, M})) \\
&= \text{Low}
\end{aligned}$$

$$\begin{aligned}
&\text{Task two risk} = \\
&\quad \text{Max}(\, f(\text{Sys3 Likelihood, Sys3 Impact}), \\
&\qquad f(\text{Sys4 Likelihood, Sys4 Impact})) \\
&= \text{Max}\ (\, f(\text{H, H}),\ f(\text{H, L})) \\
&= \text{High}
\end{aligned}$$

$$\begin{aligned}
&\text{Mission risk} = \\
&\quad \text{Max}(\, f(\text{Task One Risk, Task One impact}), \\
&\qquad f(\text{Task Two Risk, Task Two impact})) \\
&= \text{Max}\ (\, f(\text{VL, H}),\ f(\text{H, VH})) \\
&= \text{Very High}
\end{aligned}$$

As we can see from our calculations and depicted in Figure 5, the risk to Task One is Low and the risk to Task Two is high resulting in a Very High risk to our overall mission. It's important to have transparency to why there is a risk to a mission. A mission owner wants actionable data to be able to make a decision regarding their mission. Using this methodology, you are able to say "There is a high risk to the mission Task Two based on CVE-2016-4117 on System Three which is being targeted by HIDDEN COBRA botnet and CVE-2017-0144 on System Four which is being targeted by Petya Ransomware. I recommend fixing these vulnerabilities before proceeding with the mission." To be able to clearly generate that statement, our system pulls together the active threats and persistent threats and displays them to help clarify why these threats and vulnerabilities are causing risk.

4.1 Additional Considerations

The risk model proposed above follows DoDIN-RAM and uses a mission oriented assessment approach. However, there are many different risk models that could be used to calculate risk. Using this model, a single critical vulnerability can propagate up and cause a high risk score. In some organizations, it may unfeasible to remediate all vulnerabilities or they may want to look at a vulnerability threshold to assign a vulnerability score. For example, you could assign 100 points per critical, 75 points per high, 50 points per medium and 25 points per low vulnerability. Then the vulnerability score can be an aggregate of vulnerability totals (>500 = VH, >300 = H, >100 = M, >0 = L, 0=VL).

As mentioned above, DoDIN-RAM scores likelihood as a dependent variable of vulnerability and threat factors. However, there may be more complexities to consider in our likelihood assessment based on how accessible the vulnerable target may be to an adversary. For example, if the host is public facing and has critical vulnerabilities, the likelihood it is compromised is a lot higher than if it is behind a firewall or is a standalone system. This can be looked at as a cybersecurity factor which accounts for security mechanisms in place to decrease the likelihood of a successful attack. Expert judgement would have to be used to assign a rating to this factor and it can be averaged with the other likelihood calculation to either increase or decrease the likelihood. $\mathit{Likelihood} = \mathit{Avg}(\, f\,(\mathit{vulnerability},\ \mathit{threat}),\ \ \mathit{Cybersecurity\ \ level}).$

A way to increase the fidelity of the mission impact assessment is to capture impact on confidentiality, integrity and availability for each node in the mission mapping graph. It could be the case that a breach of integrity causes a very high impact and a breach of availability only causes a medium impact. If this was the case, a vulnerability that causes loss of availability would be less severe than one that causes loss of integrity. Since CVSS captures impact to each of the three security tenants, logic could be added into your risk functions to account for this.

5. Limitations and Future Work

We recognize that there are many complexities to risk; this framework is not all encompassing; however, it takes the concepts from DoDIN-RAM and NIST Special Publication 800-53 and applies it to our mission mapping tool. This model specifically uses a mission-oriented analysis approach so risk is framed in the context of mission execution. Function *f* for any of the risk factors is extensible and can be defined based on the organization's risk model. It would be possible to translate this qualitative risk assessment into a quantitative or semi-quantitative risk assessment by measuring threat and mission impact numerically rather than categorically. The benefit of this would be the factors could be weighted differently and the *f* function could be more customizable. However, since threat and mission impact are partially subjective, using categorical ranges is often easier to assess.

One area of future research could be automatically calculating a threat score based on available information. Manual assessment is currently the most widely used technique but it is a subjective and resource intensive process to perform threat assessments and assign a score. As threat sharing resources evolve, formatting intelligence in a standard structure such as STIX can help increase the fidelity of automated threat assessment tools which can lead to dynamic and automated risk assessment. Additionally, tying threat information and indicators into network sensors can help warn of threat activity earlier in the cyber kill chain.

An additional topic of interest is how to evaluate a risk model. If your risk assessment shows you have high risk for every mission but no cyber event occurs which impacts the mission, then it is possible some value is weighted too highly. If an organization recorded all cyber incidents with their threat actor and target, if known, this data could be analyzed over time to help build more accurate threat profiles and risk models. Currently, data such as this is highly sensitive and was not available for consideration in this paper.

We are continuing work on implementing a risk assessment framework into a mission mapping and cyber situational awareness tool. A shortfall of most existing mission mapping tools is they do not have the capability of performing a risk assessment.(Guion and Reith, 2017a) Ultimately, identifying risk areas is the information that decision makers are most interested in. The ability of a mission mapping tool to perform this function would increase its versatility and value to an organization.

6. Conclusion

Within the DoD, cyber risk assessments are not often conducted with emphasis on the mission. If they are conducted on a specific mission, the result is a static risk assessment report which is only useful for a limited period of time. In order to best provide mission assurance, efforts should be focused to mitigate vulnerabilities that provide the highest risk to executing missions. We proposed dynamically applying the DoDIN-RAM to continuously provide situational awareness of where risks to the mission lie. We've demonstrated how to gather sources and calculate the four risk factors and how they come together to produce overall risk to a mission. While there is work that can be done to increase the fidelity of the risk assessment, we believe this work can be a foundation or motivate future research in dynamic and mission-centric cyber risk assessments.

7. References

DoD Defense Science Board (2013) 'Resilient Military Systems and the Advanced Cyber Threat'.

FIRST (2017) 'Common Vulnerability Scoring System v3.0: Specification Document (v1.8)'. Available at: https://www.first.org/cvss/specification-document.

Guion, J. and Reith, M. (2017a) 'Cyber Terrain Mission Mapping Tools and Methodologies', in *International Conference on Cyber Conflict U.S.* Washington, D.C.

Guion, J. and Reith, M. (2017b) 'Dynamic Cyber Mission Mapping', in *Annual Industrial and Systems Engineering Conference & Expo (IISE).* Pittsburgh.

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S. and Frye, J. (2012) 'Cyber Threat Metrics'. Sandia National Laboratories.

NIST (2012) 'NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments'. Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

NIST (2013) 'NIST Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations'. Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r4.pdf.

Struse, R., Jordan, B., Piazza, R. and Wunder, J. (2017) 'STIX 2.0 Specification (version 2.0-rc2)'. OASIS Cyber

Threat Intelligence. Available at: http://stixproject.github.io/stix2.0/stixdocs/stix-v2.0-wd02.pdf.

U.S. Cyber Command (2017) 'Department of Defense Information Networks Risk Assessment Methodology Guideline. Version 2.0'.

U.S. Department of Defense (2015) 'The Department of Defense Cyber Strategy'. Available at: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Appendix A. DoDIN-RAM qualitative functions (U.S. Cyber Command, 2017)

Likelihood *(f)*		**Vulnerability**				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Threat	**Very High**	M	M	H	H	VH
	High	L	M	M	H	H
	Medium	L	L	M	M	H
	Low	VL	L	L	M	M
	Very Low	VL	VL	L	L	M

Risk *(f)*		**Mission Impact**				
		Very Low	**Low**	**Medium**	**High**	**Very High**
Likelihood	**Very High**	VL	L	M	H	VH
	High	VL	L	M	H	VH
	Medium	VL	L	M	M	H
	Low	VL	L	L	L	M
	Very Low	VL	VL	VL	L	L