Mission Models for Cyber-Resilient Military Operations

Steven Noel[*], Tim Dudman[†], Pierre Trepagnier[‡], and Sowdagar Badesha[†]

[*]The MITRE Corporation, McLean, VA, USA
[†]Riskaware, Bristol, UK
[‡]MIT Lincoln Laboratory, Lexington, MA, USA

snoel@mitre.org, [tim.dudman, sowdagar.badesha]@riskaware.co.uk, ptrepagnier@ll.mit.edu

ABSTRACT

This chapter examines the role of mission models for analyzing and improving cyber resilience in tactical military environments, and for maintaining situational understanding in the face of cyberattacks. While considering the interdependencies of mission functions and how they rely on cyber assets is fundamental to effective resilience, more work is needed in automated methods for building such dependency models. This is complicated by the fact that such dependencies often vary over time. We discuss the need for appropriate modeling abstractions and level of detail, driven by mission requirements. We also describe some preliminary efforts in standardization of mission models for cyber resilience.

1.0 MISSION MODELS AND RESILIENCE

In general, cyber resilience is a property of individual systems, system-of-systems, networks, or organizations [1]. Understanding cyber risks is a key enabler for achieving appropriate levels of resilience. Because of rich interdependencies among all levels of military activities (operational, tactical, and strategic), cyber risk is not solely determined by individual hosts, vulnerabilities, events, mission functions, etc. Rather, it is an emergent property that depends on dependencies among entities at all levels of military command and operations. Another dimension of resilience is flexible system components that manage cyber risk by changing configuration and organizational stance, such as modifying boundaries as a reaction to attack, changing roles to meet dependency needs of downstream assets, or forming new communication channels.

Because of the challenges and costs of assessing and improving resilience across a military organization, such activities should be aligned to specific mission requirements. There is a need to identify or discover the various elements that contribute to mission success, and how those elements depend upon each other. This includes (a) high-level mission objectives, (b) the operational tasks that help meet each objective, (c) the system functions that support each task, and (d) the cyber assets that enable each system function. Given the various operational threats and associated risks, such mission dependency models (e.g., graph-based) can guide remediation actions, determine appropriate system redundancies and service diversity, etc. [2]. Then, as situations involving cyberattack unfold, mission models can help prioritize alerts, assess elevated mission risk, and understand options for responding to attacks [3] [4] [5]. In terms of military doctrine, mission modeling should be considered part of Intelligence Preparation of the Battlefield (IPB) [6].

However, in the current state of practice, developing and continually maintaining mission models remains an expensive process. It might be appropriate to capture some higher-level elements of doctrine through manual efforts [7]. But because of continual churn at more operational levels, this becomes untenable for lower-level mission elements, especially in tactical environments. As an example, manual methods for producing dependency models from mission threads are expensive and unrepeatable. While there has been some progress in automated methods for mission modeling [8] [9], there has been relatively little work in this area for tactical environments. Thus, military personnel are continually challenged with understanding how cyberattacks can put missions at risk and impact performance.

2.0 RESILIENCE AS A TIME-BASED PROBLEM

Resilience is inherently a time-based problem [10] [11]. For example, maintaining operational tempo in cyberspace requires synchronizing ongoing analysis with incoming data (e.g., alert streams). At the other end of temporal relevance is the need for aging out data that are no longer relevant to mission components being protected. Another requirement for cyber resilience is to bring attention to situational changes of relevance to mission assurance, such as deviation from planned versus actual events. For example, such requirements can be addressed through dynamically changing mission-dependency graphs, with re-planning during live missions and activating alternate graph sections in response to events. A system like this could suggest changes that result in more resilient mission graphs, e.g., algorithms that run high impact/low probability analysis.

2.1 Time-Based Dependencies

Cyber resilience is quantified by the length of time necessary to recover from a perturbation. In this section, we explore another aspect of time dependence, in which the assets on which a mission depends themselves change over time. Let's explore a toy example taken from the Munich public transportation authority: returning to the Munich airport after the IST-153 Cyber Resilience Workshop. For a specific taxonomy here, we stipulate "Get to the Airport from University of the Bundeswehr" to be a sub-mission of the Tactical Mission "Attending the IST-153 Cyber Resilience Workshop," and that tactical mission to be part of the Operational Mission "My Publications in 2017," which in turn is part of the overarching Strategic Mission "My Successful Career in Cyber Security."

As shown in Figure 1, the tactical sub-mission "Get to the Airport from University of the Bundeswehr" contains a baseline Course of Action: Take Bus 199 from the University gate to the subway station, then take subway U-5 to the Ostbahnhof, then take S-Bahn 8 from Ostbahnhof to the airport. At the baseline level, mission success depends on the successive availability of the Bus 199, U-5, and S-8 assets. Each of these could be considered as sub-sub-missions of "Get to the Airport from University of the Bundeswehr," which in turn is a sub-mission of our tactical mission "Attend the IST-153 Workshop."

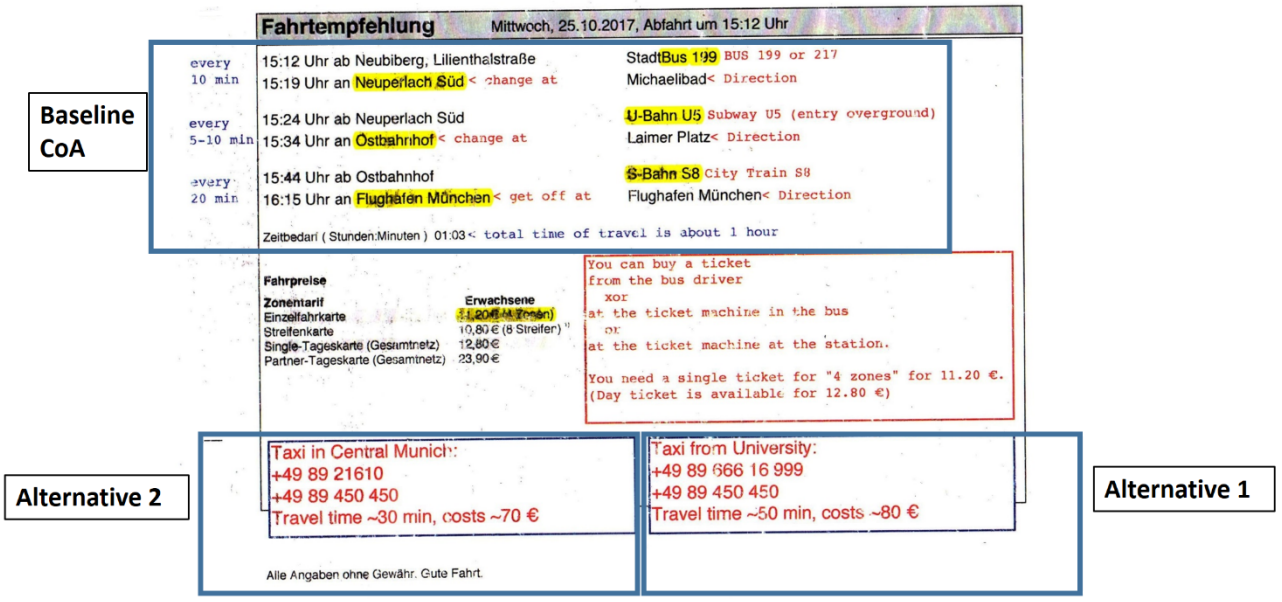

Figure 1. "Get to the Airport" Sub-Mission

Note that Alternative 1, Taxi from the University, provides resilience in case the bus or U-5 are unavailable, while Alternative 2, Taxi in Central Munich, would apply in case you have made it to Ostbahnhof, but the S-8 is not available.

The point to emphasize here is the time dependence of the supporting assets regarding their contribution to mission resilience and mission success. Once you make it to the subway station, the mission dependency on Bus 199 drops out. Similarly, once at Ostbahnhof, U-5 dependency ceases, as does the contribution of Alternative 1 to mission resilience.

2.2 Hierarchical Decomposition

The above discussion suggests a general principle: that, analytically, it makes sense to continue to decompose missions hierarchically until you get to atomic units where asset dependence is constant over time. (In the sense that your Airport mission dependence on Bus 199 is constant from the moment you step onto it until you alight at the subway station, and then vanishes.)

We suggest that it also has implications for information filtering. The exact schedules, fares, and phone numbers which the Munich transportation authority has so helpfully provided in Figure X become irrelevant once you have successfully made it to the airport, and need not be passed on up to the next higher level of abstraction. Similarly, the entire process of getting home would be unlikely to be included in a trip report discussing the tactical mission "Attending the IST-153 Cyber Resilience Workshop," and that tactical mission might get only a summary mention in the operational mission "My Publications in 2017," which in turn is subsumed in one's strategic mission "My Successful Career in Cyber Security." Thus, one can avoid the drowning in data issue which would result in retaining the fact at all levels of abstraction that a 4-zone train ticket in Munich costs 11.20 Euros.

2.3 Capability Gap

Current methods for assessing mission dependency lack both the granularity and fidelity to apply the hierarchical decomposition approach discussed above, and more particularly, the discovery of the level of granularity necessary to answer a specific question. Rather than being data-driven, they tend to rely on documentation and the memories and opinions of Subject Matter Experts. Given constant fixes and patches that occur in cyber, they tend to reflect some combination of the as-designed and as-understood structure, rather than the structure which actually exists at any given time. Developing an accurate method of actually assessing the asset dependencies of a mission, particularly with respect to timescale, is currently a significant unmet need.

3.0 APPROPRIATE MODELING ABSTRACTIONS

When constructing mission models, the model modalities and levels of abstraction need to be matched to the operational use cases. Models need to be sufficiently expressive for answering the required analytic questions and for communicating results within an organization. Indeed, as a key part of system resilience, the human element can be included for modeling decisions in response to cyber events. The level of detail needs to be appropriate for the echelon of command, along a spectrum from operational, tactical, and strategic decision making. An important research direction is to develop visual analytics and dashboards appropriate for different command levels.

Mission models based on directed acyclic graphs are built with the Cyber Command System (CyCS) tool [12], and analysed/visualized via the CyGraph tool [7]. This captures a hierarchy of dependencies (directed acyclic graph) among mission functions, the information needed for these functions, the services that provide the information, and the hosts on which the service reside. In this way, incorporating mission dependencies supports resilience by prioritizing exploitable paths that lead to mission-critical cyber assets [5]. Cyber resiliency

techniques via CyGraph [13] are augmented through information on cyber threats, vulnerabilities, policies, and traffic patterns.

An alternative approach is to create mission models that link cyber assets to organizational business processes [10] [14], employing Business Process Modeling Notation (BPMN) [15] integrated with network-attack and mission-dependency graphs. Mission process models have also been integrated with information infrastructure, with validation and reasoning provided via ontology language [16].

4.0 A COMMON MISSION MODELLING LANGUAGE

A key research direction is to develop standard taxonomy for inferring mission dependencies, risks, and impacts (including resilience parameters) based on empirical studies. For example, this might include inferring recovery time of assets through system complexity indicators (sub-component count, number of frameworks, users assigned to that component or process), asset value (cost) impact, data requirements for assets, or the presence of redundancy. This research direction dovetails with other forms of cybersecurity standardization [17]. Furthermore, the results of mission resilience analysis need to be effectively communicated to commanders, integrated through standard tactical dashboards, and mapped to geographic location as appropriate.

For assessing mission resilience to cyberattack and communicating analytic results to military commanders, a common mission modelling taxonomy and language are needed, which represent both mission vignettes and cyber entities. Standards such as Coalition Battle Management Language (C-BML) [18] define information (orders, plans, reports, requests, etc.) that can be readily processed by Command and Control (C2) systems, simulation systems, or interfaces to automated forces. Serving as an interoperability standard based on eXtensible Markup Language (XML) [19], the focus of C-BML is to convey a commander's intent. Other efforts (in both the US and UK) have focused more on developing a Cyber Mission Impact Assessment (CMIA) modelling standard for representing mission dependencies, risks, and impacts.

There are currently two CMIA standards that both allow the mission impact of potential cyberattacks on large military socio-technical systems of systems in to be modeled:

1. The US approach [10], developed by MITRE and based on BPMN, allows for explicit modeling of temporal resilience characteristics and information resources within a general-purpose approach that can compute Measures of Effectiveness (MOE) at a mission level for specific categories of cyber impacts. This approach requires manual intervention to alter the mission model to reflect the cyber effect of the incident, and repeated runs of the simulation to reflect the normal variations in mission instances.

2. The UK approach [20], developed by Dstl in collaboration with RJD Technology and based on Unified Modelling Language (UML) [21], focuses on capturing networks of Computer Information System (CIS) elements and defining mission device associations with critical mission components, termed Operational Technology (OT). Analysis scripts allow for the identification of highly connected (and therefore potentially critical) systems, potential attack paths between attack surfaces and critical systems, and the impact on business processes of a successful cyberattack. This approach was developed to support the analysis of individual military platforms and Critical National Infrastructure (CNI) as part of Cyber Vulnerability Investigations (CVI), and therefore requires an integration architecture to support analysis across multiple CMIA models to represent whole military deployments and cyber terrain. However, it does lend itself to the re-use of individual models to reduce the overall modelling burden.

The question of how to present the analysis results to mission operators has not been addressed in either the UK or US CMIA programs, and in both cases the outputs of the analysis are highly dependent on the skills and knowledge of the CMIA analyst and the availability and accuracy of the technical information used to construct the models.

In the UK, the Joint User cyber Mission Planning (JUMP) program [22] is developing a concept demonstrator to combine some of the above modelling concepts with advanced cyberattack and Mission Impact Assessment (MIA) analysis algorithms, to allow tactical military personnel to plan and conduct missions involving cyber operations. In addition, the latest user interaction and visualization technologies are being trialed to effectively capture a commander's intent through a tactical map-based dashboard and to communicate the results of analysis to military personnel at different levels.

Mission vignettes, and computer networks (including software and vulnerabilities) are being modelled as a unified, scalable connected property-graph, allowing mission dependencies and resilience parameters to be explicitly modelled at varying Levels of Detail (LOD), as well as the application of MIA methods designed to assess cyber resilience [23]. UK CMIA model interoperability is being integrated to support the automatic generation of mission vignettes comprising OT (critical mission components) for previously modelled military systems. The vignette is augmented with mission objectives and effects as military personnel interact with the variety of interfaces available to create and assess courses of action. Entire computer networks are imported separately from Network Information Systems (NIS), so device associations are required to enable detailed automated cyber resilience analysis. Joint military symbology [24] has been extended to show the location of cyber entities (e.g., unknown entities, friendly defensive cyber sections, and hostile offensive cyber squads) in familiar NATO format.

Further research is needed for the reuse of existing system models and extensions to existing symbology. Questions about improved modelling of the human element of a cyberattack and deriving detailed temporal resilience parameters in a tactical situation also need to be addressed. Any common mission modelling language must include the required elements to capture the commander's intent, OT, mission dependencies, computer networks, resilience parameters and support the necessary analysis, whilst minimizing information requirements in a tactical setting. The development of a unified CMIA modelling language could provide systems that utilize property-graph analysis techniques with detailed mission modelling system and effects templates at varying LOD, and also support advanced human-centric cyberattack and mission impact assessment techniques. Further research is also required into the LOD that would be required of such models to support the different levels of command.

5.0 SUMMARY AND CONCLUSIONS

In this chapter, we examine the role of mission models (e.g., mission-dependency graphs) for cyber resilience in military environments. Such models provide a framework that focuses resilience efforts on assuring missions, and provide mission-centric context for situational understanding in the face of cyberattacks. In terms of strategic directions for future research and development, it is important to consider automated methods for building such dependency models, to help reduce costs. Because resilience in cyberspace is inherently a time-dependent problem, mission models need to incorporate the dynamic nature of mission dependencies and network environments. Furthermore, the modeling abstractions and levels of detail need to be driven by mission requirements. Standardization efforts in the area of mission models for cyber resilience can also help in reducing costs and improving modeling accuracy and consistency.

6.0 REFERENCES

[1] D. J. Bodeau and R. D. Graubart, "Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines," January 2017. [Online]. Available: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf.

[2] S. Noel and S. Jajodia, "Metrics Suite for Network Attack Graph Analytics," in *9th Annual Cyber and Information Security Research Conference (CISRC)*, Oak Ridge National Laboratory, Tennessee, 2014.

[3] S. Noel, E. Harley, K. H. Tam and G. Gyor, "Big-Data Architecture for Cyber Attack Graphs: Representing Security Relationships in NoSQL Graph Databases," in *IEEE Symposium on Technologies for Homeland Security (HST)*, Boston, Massachusetts, 2015.

[4] S. Noel, E. Harley, K. H. Tam, M. Limiero and M. Share, "CyGraph: Graph-Based Analytics and Visualization for Cybersecurity," in *Cognitive Computing: Theory and Applications, Handbook of Statistics 35*, Elsevier, 2016.

[5] S. Musman and S. Agbolosu-Amison, "A Measurable Definition of Resiliency Using "Mission Risk" as a Metric," The MITRE Corporation, Technical Report MTR140047, 2014.

[6] Headquarters, Department of the Army and Headquarters, United States Marine Corps, "Intelligence Preparation of the Battlefield/Battlespace," Army Techniques Publication ATP 2-01.3 / Marine Corps Reference Publication MCRP 2-3A, Washington, DC and Quantico, Virginia, 2014.

[7] W. Heinbockel, S. Noel and J. Curbo, "Mission Dependency Modeling for Cyber Situational Awareness," in *NATO IST-148 Workshop on Cyber Defence Situation Awareness*, Sofia, Bulgaria, 2016.

[8] S. Musman, Automagical Dependency Mapping, The MITRE Corporation, 2017.

[9] A. Schulz, D. O'Gwynn, J. Kepner and P. Trepagnier, "Dynamically Correlating Network Terrain to Organizational Missions," in *NATO IST-153 Workshop on Cyber Resilience*, Munich, Germany, 2017.

[10] S. Musman, A. Temin, M. Tanner, R. Fox and B. Pridemore, "Evaluating the Impact of Cyber Attacks on Missions," *M&S Journal,* Summer 2013.

[11] P. Trepagnier and A. Schulz, "Mission Assurance as a Function of Scale," in *NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact*, Istanbul, Turkey, 2015.

[12] The MITRE Corporation, "Cyber Command System (CyCS)," [Online]. Available: http://www.mitre.org/research/technology-transfer/technology-licensing/cyber-command-system-cycs. [Accessed 31 May 2017].

[13] S. Noel, D. Bodeau and R. McQuaid, "Big-Data Graph Knowledge Bases for Cyber Resilience," in *NATO IST-153 Workshop on Cyber Resilience*, Munich, Germany, 2017.

[14] S. Noel, J. Ludwig, P. Jain, D. Johnson, R. K. Thomas, J. McFarland, B. King, S. Webster and B. Tello, "Analyzing Mission Impacts of Cyber Actions (AMICA)," in *NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact*, Istanbul, Turkey, 2015.

[15] Object Management Group, "Business Process Model and Notation (BPMN)," 2011.

[16] A. Barreto, P. Costa and E. Yano, "A Semantic Approach to Evaluate the Impact of Cyber Actions to the Physical Domain," in *7th International Conference on Semantic Technologies for Intelligence, Defense, and Security*, 2012.

[17] R. Martin, "Making Security Measurable and Manageable," *CrossTalk: The Journal of Defense Software Engineering,* September/October 2009.

[18] North Atlantic Treaty Organisation (NATO) Research and Technology Organisation (RTO), "Coalition Battle Management Language (C-BML), NMSG-048 Final Report," RTO Technical Report TR-MSG-048, 2012.

[19] Simulation Interoperability Standards Organisation (SISO), "Standard for: Coalition Battle Management Language (C-BML) Phase 1," 2013.

[20] C. Lang and B. Madahar, "Understanding the Mission Impact of a Cyber Attack in a System of Systems Environment," in *NATO IST-153 Workshop on Modelling and Simulation S&T: Critical Enabler for Cyber Defence*, Portsmouth, GBR, 2017.

[21] Object Mangement Group, "OMG Unified Modeling Language (OMG UML)," March 2015.

[22] A. Waldock, T. Dudman, S. J. Harold and S. Barrington, "JUMP: Concept Demonstrator for Cyber Mission Planning," in *NATO IST-156 Workshop on Modelling and Simulation S&T: Critical Enabler for Cyber Defence*, Portmouth, GBR, 2017.

[23] T. Dudman, A. Waldock and S. Barrington, "JUMP: Modelling and Simulation of Cyber Resilience for Mission Impact Assessment," in *NATO IST-153 Workshop on Cyber Resilience*, Munich, Germany, 2017.

[24] "Interface Standard: Joint Military Symbology," MIL-STD-2525D, 2014.