Mission Assurance as a Function of Scale

Pierre Trepagnier and Alexia Schulz

Cyber Systems and Operations
MIT Lincoln Laboratory
Lexington, MA 02420

***Abstract*—Since all Department of Defense (DoD) missions depend on cyber assets and capabilities, a dynamic and accurate cyber dependency analysis is a critical component of mission assurance. Mission analysis aims to identify hosts and applications that are "mission critical" so they can be monitored, and resources preferentially allocated to mitigate risks. For missions limited in duration and scale (tactical missions), dependency analysis is possible to conceptualize in principle, although currently difficult to realize in practice. However, for missions of long duration and large scale (strategic missions), the situation is murkier. In particular, cyber researchers struggle to find technologies that will scale up to large numbers of hosts and applications, since a typical strategic DoD mission might expect to leverage a large enterprise network. In this position paper, we argue that the difficulty is fundamental: as the mission timescale becomes longer and longer, and the number of hosts associated with the mission becomes larger and larger, the mission encompasses the entire network, and mission defense becomes indistinguishable from classic network defense. Concepts generally associated with mission assurance, such as fight-through, are not well suited to these long timescales and large networks. This train of thought leads us to reconsider the concept of "scalability" as it applies to mission assurance, and suggest that a hierarchical abstraction approach be applied. Large-scale, long duration mission assurance may be treated as the interaction of many small-scale, short duration tactical missions.**

I. Introduction

The Department of Defense (DoD) recognizes that all defense missions today depend on cyber infrastructure. The 2010 Quadrennial Defense Review finds that [7] "A failure by the Department to secure its systems in cyberspace would pose a fundamental risk to our ability to accomplish defense missions today and in the future." The role of cyber dependencies in providing mission assurance has inspired multiple studies and technology development efforts [2], [4], [5], [6], [8], [9]. The DoD must be able to guarantee that it can continue accomplishing critical missions, even in the face of degraded or disabled cyber infrastructure. Identifying the Cyber Key Terrain (C-KT), i.e. those cyber assets necessarily used in mission execution, is a vital ingredient needed to provide such guaranteed mission assurance. [1]

There is a divide in the literature regarding the best strategy for identifying the C-KT of a particular mission, and mapping out its network dependencies. Methodologies tend to fall in one of two basic classes: process driven mapping and artifact driven mapping. Process driven mapping makes heavy use of subject matter experts, and is typically manual and time consuming. Artifact driven mapping leverages usage data and lends itself more readily to automation, but the data frequently lacks sufficient context to reliably identify the C-KT. The proponents of both methodologies are concerned with the ability to scale up to enterprise-scale networks. Of particular concern is that dependency maps of large numbers of hosts, over very long timescales, tend to be difficult to convey succinctly. They often produce a deluge of data which suffers from the "hairball" problem when visually represented.

DoD missions can exist at the strategic, operational or tactical levels. In general, strategic and operational missions are conducted over longer timescales, and are much broader in scope than tactical missions. In this position paper we explore the hypothesis that strategic and operational missions are dependent on, and to a great degree comprised of, sub-missions conducted at the tactical level. Thus effective mission assurance at every layer of the hierarchy depends on the ability to map tactical level missions with fidelity. This is particularly pertinent to the cyber domain. It may be misguided to focus entirely on techniques and visualizations that scale up to enterprise network scale, or are capable of processing data volumes from extended periods of time. Indeed such techniques may over-aggregate and not provide sufficient situational awareness to identify and mitigate risks to the mission.

Although this discussion takes place in the context of the DoD, all of the conclusions can be generalized to apply to the civilian arena. All large organizations include missions that can be described as tactical, operational and strategic.

II. Timescale

Strategic, operational and tactical missions are conducted over distinct characteristic times. Strategic missions capture the essential role of the organization; e.g. the mission of DoD is to provide the military forces needed to deter war and to protect the security of our country [1]. Because of this, strategic missions are executed continuously rather than on a short timescale, and the mission definition evolves very slowly if at all. In contrast, tactical missions tend to comprise a specific set of military actions with a well defined goal that is easily measured; e.g. conduct an airstrike against a particular target. The duration of tactical missions is generally short, although the mission can be repeated multiple times. Tactical missions are defined and executed based on specific military actions that need to be taken, so the mission definitions are variable and are often not known in advance. Finally, operational missions involve resource allocation and the integration of tactical missions to achieve strategic ends [3]. The timescales for operational missions are generally long, but the mission definition may evolve more swiftly than that of a strategic mission.

[1] The DoD definition of key terrain in general is "Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant." The cyber version of this would also include assets that enable the adversary to execute its mission against the U.S. For the purposes of this paper, however, we have adopted a more restrictive definition focused on mission assurance.

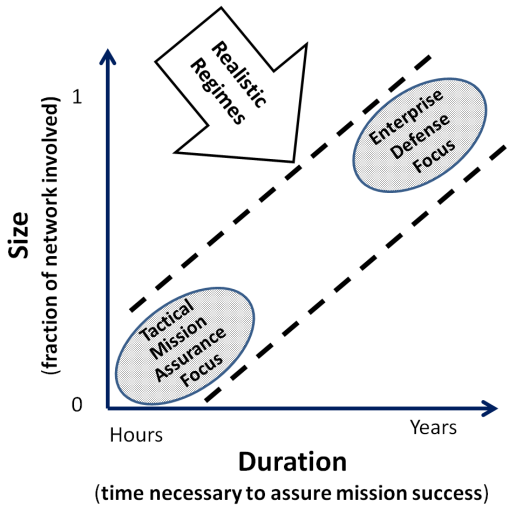


Fig. 1. *Figure 1. Tactical mission assurance involves relatively few hosts and short timescales; enterprise defense involves many hosts and long to indefinite timescales.*

According to USAF doctrine, while the resulting effects may be described as operational or strategic, military *actions* occur almost entirely at the tactical level [3]. This is particularly true in cyberspace. While cyber assets are frequently used to provide information and command and control in support of strategic and operational missions, the delivery of information, key applications, services, and command channels occurs entirely at the tactical level. This fact generates an argument for shifting the focus of dependency mapping efforts to providing mission assurance at the tactical level.

Another reason to make this shift is that certain central elements of mission assurance are easier to define and measure at the tactical level than at the operational or strategic levels. The ability to "fight through" a contested cyberspace is a concept that only applies for missions of finite duration; one cannot fight through to infinity.

III. Number of Hosts

Strategic and operational missions use a larger fraction of the total hosts on the network than tactical missions. Indeed, an enterprise network exists to serve the strategic missions of the organization. In contrast, tactical missions are generally supported by a small fraction of total network. Good network hygiene dictates that if a host is not supporting any organizational mission, it needlessly presents extra attack surface to adversaries and should be removed. But network hygiene is distinct from mission dependency mapping; the central aim of mission dependency mapping is to identify a restricted set of hosts (as a fraction of total network) critical to a particular effort. If the number of hosts necessary to prosecute a mission approaches the size of the network, mission defense is indistinguishable from classic network defense. In practice, number of hosts and timescale (discussed above) are correlated, depicted schematically in Figure 1.

Another central element of effective mission assurance at the operational and strategic levels incorporates well defined Courses of Action (COAs) designed to help decision makers react to evolving priorities and risks. Mapping the COA dependencies independently is critical. In a contested cyber environment one cannot defend every asset. Limited resources need to be allocated to defend highest priority cyber terrain, based on tactical decisions regarding which COA is being pursued in support of the operational or strategic mission.

IV. Discussion

The import of the arguments presented here is that mission assurance software need not "scale" to the size of a global enterprise, as the term scaling is usually defined. Visualizations and algorithms need not work for thousands of hosts. If thousands of hosts are present in the dependency map of an operational or strategic mission, with little or no fidelity in the mapping of the tactical importance of these hosts, it will be difficult for mission defenders to know which hosts should be monitored. Such a dependency map will not help them correctly prioritize the allocation of resources, rather it will be an illegible hairball, and be ignored.

Enterprise scale mission assurance is instead achieved by hierarchical decomposition into tactical missions, each associated with a particular COA. It is important to explore the validity of modeling strategic or operational missions as entirely composed of missions at the tactical level, with the overarching mission being decomposed into sub-missions, and sub-missions decomposed into sub-sub-missions, and so forth. At each mission level, as much detail as possible of the level below is abstracted away, leaving only those details which are necessary to maintain fidelity of mission interactions. In this manner, the problems associated with scaling and data deluge are minimized. However, effective models of mission assurance for operational and strategic missions will necessarily involve retaining enough fidelity to capture the complex interactions possible between multiple tactical building blocks [10]. Determining the minimum necessary level of fidelity is an important area for future investigation.

V. Conclusions and Recommendations

In summary, we are asserting two major propositions. First, in the cyber domain, crucial mission assurance constructs such as cyber key terrain and fight-through are meaningful for tactical missions involving limited time and a small fraction total network resources, but cease to be useful for enduring missions which utilize a large fraction of cyber resources. In the latter case, mission assurance simply degenerates into classic network defense and network hygiene. Second, that large, enduring, strategic missions may in fact be decomposed hierarchically into many small tactical ones, and that by so doing problems of scaling, data deluge, and visualization (the hairball problem) are minimized by dropping complexity between layers of the hierarchy. The outstanding problem becomes determining the minimum fidelity necessary in the dependency mapping of tactical missions and sub-missions to maintain accurate models of complex system interactions between the tactical building blocks. Our recommendations are to focus near term efforts on developing technology for the swift and accurate mapping of tactical missions, with a longer term focus on modeling their complex interactions to assure larger scale missions.

ACKNOWLEDGEMENTS

The authors wish to thank Chris Degni, Jeffrey Gottschalk, and Reed Porada for helpful comments on an early draft.

This work is sponsored by the by Department of the Air Force under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

REFERENCES

[1] U. S. Department of Defense, http://www.defense.gov/about.

[2] *Camus: Automatically Mapping Cyber Assets to Missions and Users*, MILCOM 2009. IEEE, Oct 2009.

[3] *Basic Doctrine Volume 1*. Curtis Lemay Center for Doctrine Development and Education, 2011.

[4] *A systems engineering approach for crown jewels estimation and mission assurance decision making*. IEEE, April 2011.

[5] *NSDMiner: Automated Discovery of Network Service Dependencies*, IEEE International Conference on Computer Communications, Orlando, FL, March 2012. IEEE.

[6] R. Elder. Defending and operating in a contested cyber domain,". *Air Force Scientific Advisory Board, Winter Plenary*, 2008.

[7] R. Gates. *Quadrennial Defense Review Report (Feb. 2010)*. DIANE Publishing Company, 2010.

[8] E. Peterson. Dagger: Modeling and visualization for mission impact situation awareness. Manuscript submitted to 2015 IEEE International Symposium on Technologies for Homeland Security, 2015.

[9] J. Watters, S. Morrissey, D. Bodeau, and S. C. Powers. The risk-to-mission assessment process (riskmap): A sensitivity analysis and an extension to treat confidentiality issues. *The Institute for Information Infrastructure*, July 2009.

[10] W. Young and N. G. Leveson. An integrated approach to safety and security based on systems theory. *Communications of the ACM*, 57(2):31–35, 2014.