MEASURING RESILIENCY OF MILITARY NETWORKS

By Jon Thompson, Senior Operations Research Analyst and TASC Associate Technical Fellow, October 2013

Introduction
Space systems provided by U.S. Air Force Space Command (AFSPC) are critical to the nation’s ability to defend our borders and take the fight to our adversaries, wherever they are located. Without precision timing and geolocation, communications, and ISR collection, our net-centric military strategy breaks down and we lose the benefits of our superiority in these areas. Our dependency on space and other network enablers have been identified as key to our future strategy in documents such as the space commission report\(^1\) and AFSPC white papers on the need for resiliency.\(^2\) It is clear resilient space systems are essential to our military strategy.

Unfortunately, while it is easy to recognize the need for resiliency, defining and measuring it has proven difficult. General concepts such as disaggregation can help increase architectural resiliency, but by how much? Since many resiliency options also increase complexity and system cost, how can resiliency improvements be balanced with the rest of the system to provide maximum capability at minimum cost? How can resiliency efforts be targeted, and conversely, how can adversary resiliency weaknesses be located and targeted? Unless these questions can be answered, improvements to military resiliency will be difficult to design and implement. Developing a method to quantify resiliency is essential to this process. Such a measurement will not only provide a way to improve our systems, but may also provide information to assist in locating and exploiting weaknesses in adversary architectures.

Measurement Approach
To measure resiliency, it is first essential to define it. AFSPC has defined resiliency as the ability of a system architecture to continue providing required capabilities in the face of system failures, environmental challenges, or adversary actions.\(^2\) To create a measurement of resiliency, it is important to first determine some way to measure the ability of a network to provide required capabilities, then determine how network changes affect the network’s ability to provide those capabilities after improvements or degradations. So how can this be accomplished?

All networks, computer, communication, C2 flow, road, etc., can ultimately be reduced to mathematical graphs, that is, to nodes and links between nodes. Over time, methods have been developed to assess the capabilities and limitations of the structure of such graphs, and these measures can be used to evaluate network capabilities and responses to changes in the network structure. Some possible metrics that may prove useful in assessing resiliency include:

- **Redundancy**: Measures the number of possible paths data can use to move through a network. More paths provide a backup to the primary path, increasing resiliency. While the number of possible paths through a complex network can be very large, algorithms exist to efficiently calculate paths to the level of detail necessary to provide a good assessment of network capability.

- **Path Length**: Measures the length of the path a message is likely to take through a network. Longer paths have more possible points of failure and slow information flow, reducing resiliency. The average

---
\(^2\) Air Force Space Command Resiliency and Disaggregated Space Architectures White Paper
path length of a network can be useful as an overall metric of resiliency, while path lengths for individual message flows can provide information on the resiliency of a particular service or mission.

**Measures of Central Tendency:** A family of measures assessing the relative importance of nodes and links given common network message flows. PageRank is one common algorithm used for this type of assessment. Invented by Google to evaluate the importance of web pages, PageRank has proven very useful in locating critical nodes in networks of all types. By applying these metrics to current or planned networks, it is possible to gain a great deal of insight into how these networks may function both as designed, and after changes due to modifications or adversary action. This information can be used to target improvements in order to maximize a network’s resiliency at a given cost.

Some pioneering work has already been done in applying these and other metrics to military networks, and the results have been very promising. Figure 1 shows how small design changes, in this case the addition of one additional redundant signal path for a critical node, can increase a candidate resiliency metric in a notional SSA network. In this case, the metric consists of a weighted combination of redundancy and path length. Tools already exist to map networks and create these metrics, and modifications can easily be made as required to tailor the tools and metrics to the desired network capabilities. The resulting baseline analysis will provide innovative process for designing and assessing future network modifications.

It is also possible to use PageRank or other metrics to assess node criticality, providing insights on how design changes could improve network resiliency. The same process can also be used to target weak points in adversary networks. Figure 2 shows an example of a PageRank metric run on the same notional SSA architecture. The red and blue color-coding indicates node criticality, with red nodes the most critical, and blue nodes the least. Shades of color indicate nodes between these two extremes, with near-white nodes falling near the overall network average in terms of criticality. Focusing improvement efforts on the most critical nodes would allow the command to maximize capability improvement at a given cost point, or to reduce costs while minimizing the resulting loss of capability.

**Conclusion**

TASC will present a review of how using network metrics as a measure of resiliency is a useful technique for quantifying effects of architecture changes and degrades. Combinations of these metrics could be developed to establish standards for designing evaluation criteria to determine operational impacts to networks. Implementing these analysis processes could precede quickly using well established tools and processes, providing key innovations in network assessment. As knowledge and tools for this analysis grow, the process could be generalized to other networks, greatly improving our ability to protect our networks, and thus our forces while holding adversarial forces at risk.

---

3 Distributed Networked Operations: The Foundations of Network Centric Warfare, Jeffrey Cares, January 25, 2006