Research Report

RAPAPORT (Resilience Assessment Process and Portfolio Option Reporting Tool)

Background and Method

Paul Dreyer, Krista S. Langeland, David Manheim, Gary McLeod, George Nacouzi

RAND CORPORATION

For more information on this publication, visit www.rand.org/t/RR1169

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-0-8330-9209-0

Published by the RAND Corporation, Santa Monica, Calif.

Preface

Increasing the resilience of mission-essential functions enabled by space assets and their supporting infrastructure against disruption, degradation, and destruction is a stated goal of the *National Space Policy of the United States of America*.[1] However, enhancing the resilience of U.S. space capabilities must occur in a financially constrained environment. The Air Force has tasked RAND with developing a framework for identifying effective and economically feasible non-materiel measures for increasing the resilience of its space assets. As part of that effort, RAND researchers conducted a review of industry methods for evaluating the materiel elements of space resilience and used concepts from those methods to develop a process for evaluating the non-materiel resilience of a system. The process and tool we developed (Resilience Assessment Process and Portfolio Option Reporting Tool, or RAPAPORT) have broad applications to any organization seeking to enhance resilience, as well as to those specifically in the space community.[2] This research was sponsored by the commander, Air Force Space Command, and was conducted within the Force Modernization and Employment Program of RAND Project AIR FORCE as part of a fiscal year 2014 project, "Space Resilience: Developing a Strategy for Balancing Capability and Affordability with Resilience."

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the U.S. Air Force's federally funded research and development center for studies and analyses. PAF provides the Air Force with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Force Modernization and Employment; Manpower, Personnel, and Training; Resource Management; and Strategy and Doctrine. The research reported here was prepared under contract FA7014-06-C-0001.

Additional information about PAF is available on our website:
http://www.rand.org/paf/

This report documents work originally shared with the U.S. Air Force on September 25, 2014. The draft report, issued on November 18, 2014, was reviewed by formal peer reviewers and U.S. Air Force subject-matter experts.

---

[1] The White House, 2010.

[2] RAPAPORT is available at www.rand.org/t/TL184.

Contents

Figures and Table

Figures

Table

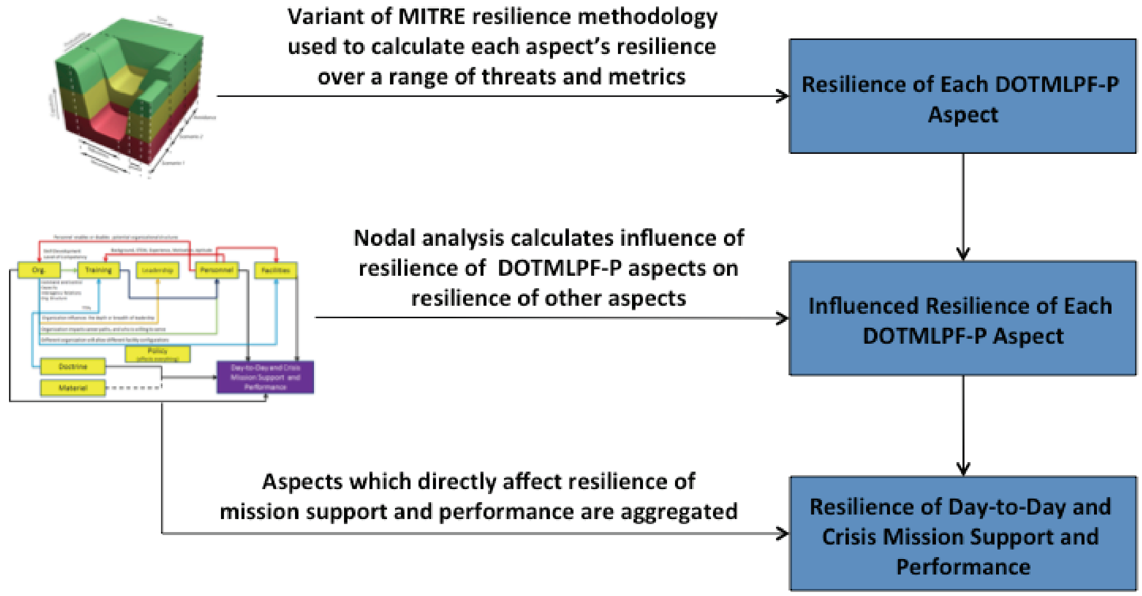
Summary

As part of the 2014 project "Space Resilience: Developing a Strategy for Balancing Capability and Affordability with Resilience," we were tasked with identifying non-materiel solutions for improving the resilience of the U.S. space enterprise and developing an analytical approach for evaluating the impacts of the potential improvements. In the military context, resilience indicates the ability of a system, architecture, or organization to maintain critical capabilities during and following a threat or disruption. Assuring resilience can be a costly endeavor, and in a financially constrained environment innovative approaches for assuring resilience are required. Often these innovative approaches lead to modifications of non-materiel aspects of a system or organization; such aspects include emergency response planning, organizational culture or structure, and training. The impact of these modifications is challenging to quantify, and ascertaining which modifications will provide the greatest impact is a challenge for Air Force Space Command and myriad other communities.

We analyzed a number of methods from industry to evaluate the resilience of the materiel element of U.S. space architecture. There were many common threads between the methods, including that they each break resilience into avoidance (the ability to avoid adverse events), robustness (the ability to withstand an adverse event as it is happening), and reconstitution and recovery (the ability to quickly regain an acceptable level of effectiveness and to eventually return to full capability). A method developed by MITRE considered these aspects of resilience both over time and over the probability space of potential adverse events. In addition, MITRE (and others) developed a framework for determining appropriate metrics for resilience, with MITRE settling on the expected availability of the required capability across multiple threats—which is the likelihood over time that for a given adverse environment the required capability level will be available—as its recommended metric for resilience.

After some deliberation, we chose the method suggested by MITRE as a starting point for our model development for calculating the resilience of the non-materiel elements of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P). This is shown in Figure S.1.

Figure S.1. Resilience Calculation Method Summary



We modified the approach by including metrics specific to each element of DOTMLPF-P under consideration and generalizing the weighting of the adverse events to include metrics without a time element. We also used relative weightings of a set of spanning test cases consisting of one or more adverse events of concern to the decisionmaker in the place of probabilistic elements. We then developed a nodal network construct to capture the interdependency of the DOTMLPF-P elements and their impact on overall resilience. We also developed a resilience calculator to evaluate portfolios of potential options to improve resilience, display results, and evaluate marginal changes to potential portfolios to determine which options provided the greatest improvement for the least cost.

Acknowledgments

We would like to thank the project's action officer, Lt Col Steve Lindemuth, chief of Architectures and Support Branch, Air Force Space Command (AFSPC/A5XA), for his assistance during the course of the project. This work also benefited greatly from extensive discussions with RAND colleagues Mel Eisman, Myron Hura, and Lara Schmidt and Air Force Fellows Col Andrew Kleckner, Col Rose Jourdan, and Col Charles Galbreath on the subject of resilience.

Abbreviations

AFSPC	Air Force Space Command
ASAT	anti-satellite (weapon)
C2	command and control
DoD	U.S. Department of Defense
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
DOTPF	doctrine, organization, training, personnel, and facilities
I&W	indications and warning
ISRD	Intelligence Surveillance and Reconnaissance Division
JSpOC	Joint Space Operations Center
MoE	measure of effectiveness
MoM	measure of merit
MoP	measure of performance
NASIC	National Air and Space Intelligence Center
NDIA	National Defense Industrial Association
OSD	Office of the Secretary of Defense
RAPAPORT	Resilience Assessment Process and Portfolio Option Reporting Tool
SME	subject-matter experts
SOPS	Space Operations Squadron
SWS	Space Warning Squadron
TTP	tactics, techniques, and procedures
USAF	U.S. Air Force

1. Introduction

Research Objective

A 2014 RAND project on space resilience, titled "Space Resilience: Developing a Strategy for Balancing Capability and Affordability with Resilience," had two main tasks: to help the Air Force identify actions that enhance space resilience through non-materiel means and to develop a method to assess the potential impacts of these actions. We created the Resilience Assessment Process and Portfolio Option Reporting Tool (RAPAPORT; available at www.rand.org/t/TL184) to address the latter of the two tasks, namely, to develop an approach that can be used to assess non-materiel aspects of resilience.

We refer to an Air Force Space Command (AFSPC) white paper for AFSPC's definition of resiliency:

> *Resiliency* is the ability of a system architecture to continue providing required capabilities in the face of system failures, environmental challenges, or adversary actions.[3]

In a separate U.S. Department of Defense (DoD) fact sheet, resilience is further separated into four aspects:

> Resilience encompasses avoidance, robustness, reconstitution, and recovery
>
> - *Avoidance*: countermeasures against potential adversaries, proactive and reactive defensive measures taken to diminish the likelihood and consequence of hostile acts or adverse conditions
> - *Robustness*: architectural properties and system of systems design features to enhance survivability and resist functional degradation
> - *Reconstitution*: plans and operations to replenish lost or diminished functions to an acceptable level for a particular mission, operation, or contingency
> - *Recovery*: program execution and space support operations to re-establish full operational capability and capacity for the full range of missions, operations, or contingencies.[4]

Research Approach

We reviewed several already existing approaches that attempted to assess the resilience of primarily materiel elements of the space mission. After some deliberation, we chose the method suggested by MITRE as a starting point for our model development. The MITRE method uses a

---

[3] Air Force Space Command, 2013, p. 2. It should be noted that *resilience* has a wider meaning it its normal English usage, in which case it refers to the ability to spring back into shape or recover from difficulties.

[4] U.S. Department of Defense, 2011.

stochastic approach analyzing adverse events and their effects on the system under consideration, with the metric being the expected ability of the system to recover sufficient capability to carry out its mission over time for each adverse event. We modified the approach by including metrics specific to each doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) element under consideration and generalizing the weighting of adverse events to include metrics without a time element. We used relative weightings of a set of spanning test cases consisting of one or more adverse events of concern to the decisionmaker, instead of event probabilities, which are unlikely to be known.[5] We then developed a nodal network construct to capture the interdependency of the DOTMLPF-P elements and their impact on overall resilience.[6] The method we developed is not specific to the resilience of space architectures and can be readily generalized to other fields.

Report Structure

In Chapter Two, we describe methods from industry that attempted to assess the resilience of primarily materiel elements of the space mission. In Chapter Three, we describe the method we developed to calculate the resilience for the non-materiel elements of DOTMLPF-P. In Chapter Four, we describe the tool that performs our resilience calculations and give a user manual for the workbook (this tool and the user manual are available at www.rand.org/t/TL184).

---

[5] There are other means of aggregating results across multiple adverse events. For example, one may want to highlight the minimum performance of the system across all adverse events considered. See Davis, 2014, for a further discussion.

[6] Because the material, leadership, and policy elements of DOTMLPF-P were outside the purview of this study, the methodology present in this document focus entirely on the remaining elements—doctrine, organization, training, personnel, and facilities (DOTPF).

2. Review of Other Methods for Measuring Resilience of Space Systems

There is an extensive literature on methods to define and evaluate resilience of systems, companies, and so forth.[7] A number of companies have developed approaches for determining the resilience of space architectures via a variety of different means. We summarize some of them below.

Boeing

In a presentation to the National Defense Industrial Association (NDIA) Resilience Forum in 2013,[8] Boeing defines resilience based on the amount of capability a system or architecture retains through a set of threat scenarios. Boeing's analysis ties back to the four aspects of resilience mentioned earlier: avoidance, robustness, reconstitution, and recovery. For a single threat, Boeing calculates four measures between 0 and 1to reflect each of these aspects ($R_{AV}, R_{RO}, R_{RC}, R_{RV}$) and then derives a single resilience value (*R*) via $R = 1-(1-R_{AV})(1-R_{RO})(1-R_{RC})(1-R_{RV})$. Treating these measures as independent probabilities, the resilience metric is essentially is the probability of avoiding, being robust against, recovering, *or* reconstituting against an attack.

In the presence of multiple threats, Boeing's method determines the cumulative system resilience against a set of threats by subtracting away all of the reductions in resilience from 1, which can result in potentially negative resilience, and no mention is made of any weighting or relative likelihood of threats. Accordingly, it becomes difficult to attach significant meaning to the values that result from the analysis.

Northrop Grumman

In a presentation to AFSPC in 2013,[9] Northrop Grumman criticizes the analytic modeling approach used by Boeing and others for using subjective numerical analysis to estimate the level of resilience in aspects such as avoidance, robustness, reconstitution, and recovery. Northrop Grumman claims that such calculations are a non-intuitive process, difficult to verify, and result in highly subjective accuracy that gives no compelling message to stakeholders. In its place, Northrop Grumman claims to have developed an objective, intuitive process that also

[7] Langeland et al., 2016.

[8] Burch, 2013.

[9] Edlund, 2013.

incorporates costs and characterizes the resilience of a system by which threats can exploit a systems weak links and cause breaking points to occur. Northrop Grumman defines a systems resilience value by the ratio of the costs of a successful threat against a system and the system's cost itself. While intuitive and tied to notions well understood by stakeholders (namely costs), the process seems tied primarily to enemy actions and ignores virtually every other aspect of resilience, such as a system's ability to resist or quickly recover from an adverse event even if it temporarily fails.

Lockheed Martin and KTSi

In separate briefings at NDIA meetings,[10] both Lockheed Martin and KTSi use a fairly standard risk-based assessment of resilience, relating it to a threat's likelihood and consequence and a system's ability to mitigate it, with KTSi using the standard 5x5 DoD risk reporting matrix.[11] Of particular interest, however, is Lockheed Martin's effort to review Office of the Secretary of Defense (OSD), U.S. Air Force, and Intelligence Community frameworks to formulate a series of potential metrics and evaluation criteria for resilience. The metrics of interest Lockheed Martin discussed were as follows:

- measure of merit (MoM):
  - ability to maintain capability against hazards and threats
- measures of effectiveness (MoEs):
  - ability to maintain objective level of capability
  - ability to maintain threshold level of capability
  - ability to diminish consequence of hazard
  - ability to restore capability
- measures of performance (MoPs):
  - extent of capability retained or lost
  - effectiveness of mitigation measure
  - alternative means to provide capability
  - time to recover
  - time to reconstitute.

In addition, Lockheed Martin developed a four-level (none, low, medium, and high capability), color-coded set of evaluation criteria for the aspects of resilience as well as the extent of the capability retained after an adverse event.

---

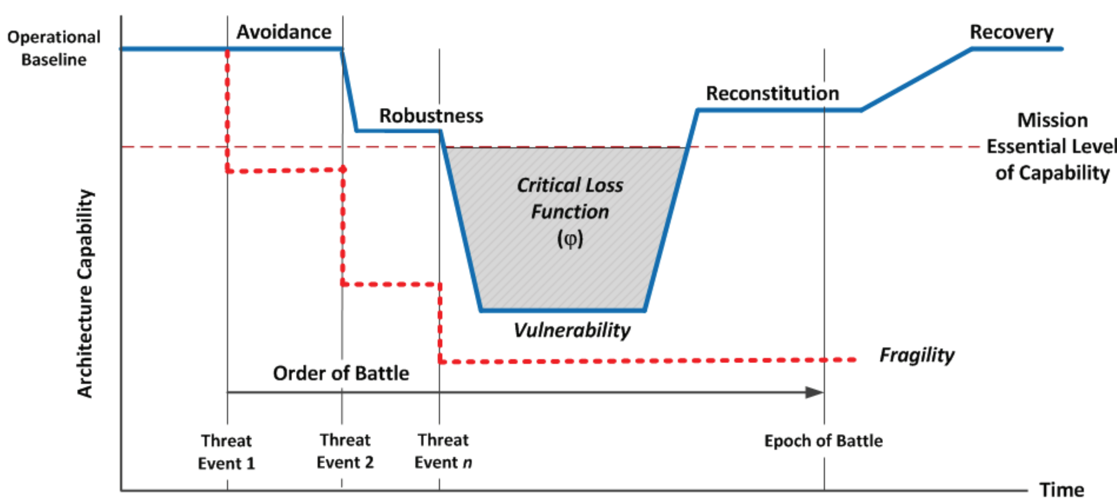
[10] Lockheed Martin, 2013; Long, 2012.

[11] See, for example, U.S. Department of Defense, Acquisition, Technology, and Logistics, 2006.

Aerospace

In a 2013 report,[12] Aerospace explicitly incorporates the magnitude and duration of the capability loss due to an adverse event into its evaluation of the resilience of a system. A sample evaluation of capability loss as a function of time from the Aerospace report is shown in Figure 2.1. Shaded in gray, the figure shows the *critical loss function*, the time-integrated loss of capability below a mission essential level of capability.[13] Over a series of adverse events (which the figure refers to as the "order of battle," which typically has a different meaning in this context), the figure also highlights the various aspects of resilience, including avoidance (capability is fully maintained because Threat 1 is circumvented), robustness (system is damaged by Threat 2, but only suffers a minor degradation), reconstitution (the time it takes to recover from being vulnerable to a mission essential level of capability), and recovery (the time it takes to recover full capability). In addition, the shape of the capability loss function is important; there are several possible shapes for the areas under the essential capability level, such as a sudden drop and reconstitution of capability, or a sudden loss with gradual reconstitution or vice versa—all three are possible modes for a system to deteriorate and recover. The Aerospace report also highlights the notion of *fragility* or *brittleness* of a system—the point beyond which there is an irreversible loss that cannot be reconstituted—as a converse to resilience.

Figure 2.1. Sample Capability Loss Function



SOURCE: Wilson et. al., 2012.

---

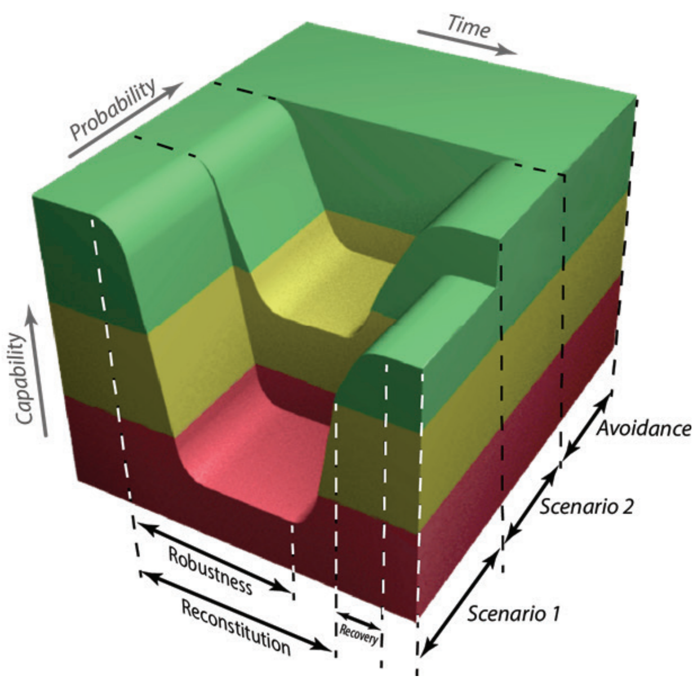
[12] Wilson, Fujita, and Nygren, 2013.

[13] This approach is fairly similar to what other parts of DoD refer to as *system agility*. For additional information, see Alberts, 2011, and Task Group SAS-085, 2014.

MITRE

In a 2013 briefing,[14] MITRE builds on the capability loss function used by Aerospace and adds the third dimension of the probability of adverse events into it, giving a three-dimensional surface with axes of time, probability, and capability and measures the resilience of a system using the volume under the capability surface when summed over the probability of all possible events (each weighted by the probability of occurrence) and integrated over time. An example of this from the MITRE briefing is shown in Figure 2.2. It shows the axes of time, probability, and capability, with green representing sufficient capability, yellow representing degraded- but-above-mission-essential levels of capability, and red corresponding to less-than-mission-essential levels of capability. Reflecting the aspects of resilience, some events are avoided entirely (corresponding to the back third or so of the volume, where the capability of the system is not decreased). The graphic also shows the notion of robustness with Scenario 2, with capability being reduced but remaining above mission-essential levels. For the adverse events in Scenario 1, the capability drops below mission-essential levels but reconstitutes and eventually recovers. In addition, MITRE correctly notes that modeling the actual capability surface may be difficult and proposes simpler curves, such as binary ones that map to 0 or 1 depending on whether or not the system is at a minimum essential level of capability.

Figure 2.2. The Probability Weighted Resilience Volume



SOURCE: Brtis, 2013.

[14] Brtis, 2013.

The MITRE study also developed the following set of questions intended to provide a framework to assess the quality of resilience metrics:

1. Does the metric address and cohere with the AFSPC definition of resilience?
2. Does the metric represent the ability to avoid adversity?
3. Does the metric represent the robustness of the item?
4. Does the metric represent the ability to reconstitute?
5. Does the metric represent the ability to recover?
6. Are the data needed for the metric obtainable?
7. Is the calculation of the metric practically feasible?
8. Does the metric avoid pathological incentives that could incent the provider to deliver the wrong thing?
9. Does the metric inform on whether minimum capability is ever violated?
10. Does the metric inform on the amount of risk that is being accepted?
11. Does the metric inform the decision maker when added resilience no longer adds value?
12. Does the metric represent the OSD guidance that a higher probability of capability indicates higher resilience?
13. Does the metric represent OSD guidance that shorter periods of reduced capability indicate higher resilience?
14. Does the metric represent OSD guidance that addressing a wider range of scenarios indicates higher resilience?
15. Does the metric allow for a spectrum of threats?
16. Does the metric represent the amount of capability degradation?
17. Does the metric represent the length of capability degradation?
18. Does the metric address the temporal component of the resilience lifecycle?
19. Can the metric support the OSD "resilience level" method?

In the end, MITRE settled on the expected availability of the required capability—the likelihood over time that for a given adverse environment the required capability level will be available—as its recommended metric for resilience. It satisfies many of the questions asked above, is relatively straightforward to evaluate provided the probabilities of the adverse events are known, and indicates whether and when the minimum capability is lost as well as when further investments in resilience stop adding value, but it does not describe how deep a loss in capability is, nor the shape of its recovery. MITRE represents the resilience metric (R) using the equation

$$R = \sum_{i=1}^{n} \left(P_i \frac{1}{T} \int_{t=0}^{T} Cr_i(t)dt \right),$$

where the set of adverse events are indexed from 1 to n, P_i is the probability of occurrence of adverse event i, and $Cr_i(t)$is the function that is 1 if the system is above the required capability level at time t, and 0 otherwise. This function is averaged over the length of the timeframe of interest T for the adverse event (hence the integral and $1/T$ term) to get the desired metric. If an event can be avoided completely or the system is robust enough to not drop below its required capability level, then we know that $Cr_i(t) = 1$ for all t.

One thing implicit in this calculation is that $\sum_{i=1}^{n} P_i = 1$; that is, the set of events (or combinations of adverse events) span all possibilities. It is unlikely, however, that any analysis would span all possibilities. Implicit in this indexing is that all adverse scenarios have been explicitly identified for consideration (or alternatively, the full set of those of interest to the decisionmaker). Alternatively, one can assume that the probabilities are conditioned on one of the adverse events happening, which has the same effect. This latter view is preferable, as otherwise an infrequent but devastating event would have a minimal impact on resilience as the system is operating at full capability most of the time. Instead, the resilience of the system is evaluated in an environment and over the period of time where it is being challenged. However, it is also likely to be difficult to estimate those probabilities accurately or consistently.

We ended up choosing the MITRE method as our starting point for calculating the resilience of some of the non-materiel elements of DOTMLPF, because it captured both the elements of time and relative weighting of events (in their case, via probability) with regard to the calculation of resilience, was relatively straightforward to calculate (provided the event probabilities are available in empirically justified data), and already had considerable traction and understanding at AFSPC. Because the probability of particular adverse events may not be known and may be impossible to calculate, we can more generally associate each event (or a set of spanning test cases each consisting of one or more adverse events) with a weighting that corresponds to its relative importance to the decisionmaker. Similarly, instead of explicitly modeling the capability loss function associated to each test case and integrating it over time, the expected availability of required capabilities (or whatever other resilience metric is appropriate for the DOTMLPF element under consideration) can be represented by a value between 0 and 1 corresponding to the amount of fulfillment of the metric. This metric does not necessarily have to be time-weighted to a particular event, as it may be the case that, for the DOTMLPF element we are considering (doctrine or training, for example), the time component of the threat scenarios is not be applicable. In that case, the metric represents the amount of fulfillment of the metric after an adverse event. Improvements to resilience can be evaluated via the amount of the gap between the current resilience metric value and 1 (or maximum resilience) that the improvement would recover, either via improving avoidance (and reducing the probability that the event has an impact) or robustness, recovery, and reconstitution (reducing the time or impact of an event to capability if it occurs).

3. A Method for Assessing Resilience

As we showed in Chapter Two, several companies developed different methods to assess the resilience of primarily materiel elements of the space mission. After some deliberation, we chose the method suggested by MITRE as a starting point for our model development for calculating the resilience of some of the non-materiel elements of DOTMLPF-P. The MITRE method uses a stochastic approach, analyzing adverse event scenarios and their effects on the system under consideration, with the metric being the expected ability of the system to recover adequate capability over time. We modify the approach by including metrics specific to each doctrine, organization, training, personnel, and facilities element under consideration and generalizing the weighting of the event scenarios and include metrics without a time element. We use relative weightings of a spanning set of test cases consisting of one or more adverse events of concern to the decisionmaker as probabilities of event occurrence are either unknown or based on the decisions of an adversary. We then developed a nodal network construct to capture the interdependency of the DOTMLPF-P elements and their impact on overall resilience.

Calculating the Resilience of a Single DOTMPLF Element

To summarize our method, we introduce some notation:

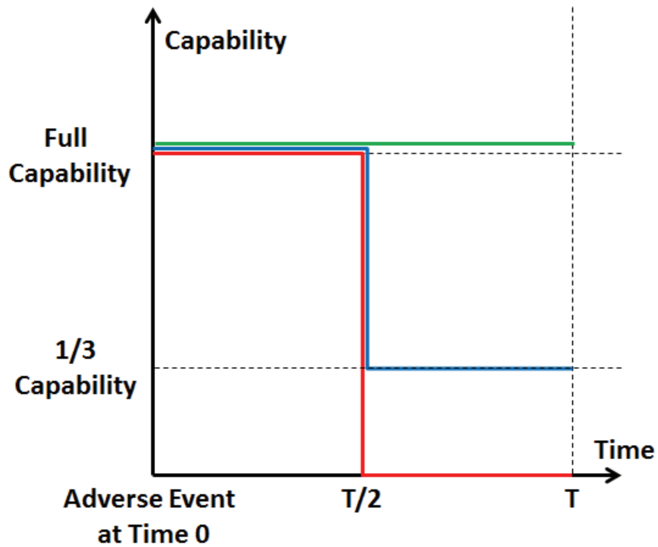
- There are four main sets of objects: elements of DOTMLPF, test cases of adverse events, options, and portfolios of options. We will index these sets in our equations by *e, i, j,* and *k*, respectively.
- We assume that there is a spanning set of test cases (each of which may contain one or more adverse events) to stress the force capabilities in all relevant ways. Our *n* test cases are enumerated $TC_1, \ldots, TC_n$, each with weighting $P_1, \ldots, P_n$ and impact $I_1, \ldots, I_n$ to the system's capability (that is, the metric being computed for a given DOTMPLF element) if the adverse events in the test case occur unimpeded (ignoring any potential resilience of the current system to the adverse event). For simplicity, we assume both the weights and impacts to be scaled to between zero and one. As a starting point, it may make sense for all weightings to be equal for the test cases. In terms of the variables of the MITRE resilience metric, the impact, I_i, over the timeframe of interest for the test case of adverse events is $I_i = 1 - \frac{1}{T}\int_{t=0}^{T} Cr(t)\,dt$, where $Cr(t)$, is the capability metric being measured.[15] As an example, for the facilities element, the metric may be the fraction of the time that the minimum mission capability of the facility is provided. If the timeframe

[15] In the case where there is no time element associated to the metric or test case, the impact is simply the amount of capability lost after the adverse event(s).

of interest in a single test case was a day and there was an adverse event (say, a power outage) that, if it occurs, shuts down operations at a facility for an hour, then the impact of that particular event would be 1/24. Note that the metric may not have a time element, in which case the impact represents the amount of the capability lost.

- The system may have some baseline resilience against the adverse events in a test case. We denote the expected amount of reduction of impact that the base can recover from the adverse events in test case TC_i with $W_{i,0}$. These values are scaled between 0 and 1, with 1 denoting that the current system never loses capability due to the adverse events in a test case. Returning to our example test case, if the facility already has a backup power generator that takes six minutes to become operational, then $W_{i,0} = 0.9$, as 54 out of the 60 minutes of outage are recovered. The determination of this value can and should reflect the aspects of resilience: avoidance, robustness, recovery, and reconstitution. Essentially, the analyst should determine the shape of the capability loss function (as in Figure 2.1), which includes all of these aspects, and integrating under that curve over time gives the baseline level of resilience.
- We are considering a series of potential options to improve the resilience of a system above and beyond the baseline. We enumerate those options with $O_1, \ldots, O_m$, each with cost $C_1, \ldots, C_m$. We denote with $W_{i,j}$ the amount of lost capability option O_j can recover from an occurrence of the adverse events in test case E_i. Again, the determination of this value can and should reflect the aspects of resilience: avoidance, robustness, recovery, and reconstitution. The analyst should determine the shape of the capability loss function (as in Figure 2.1) when this option is available, and integrating over time the curve when the option is present gives the level of capability when that option is available. The amount of capability recovered by an option is the increase in capability over the baseline divided by the capability lost when only the baseline is available. As an example, consider Figure 3.1. The red graph denotes the baseline resilience in the face of an adverse event *i*: It is able to retain capability for half of the timeframe of interest *T* for this particular test case, at which point it loses full capability. Therefore, $W_{i,0} = 0.5$. The blue graph shows the effect of an option j_1 that provides some robustness in that the capability falls to 1/3 of full capability instead of deteriorating completely. Accordingly, $W_{i,j_1} = 1/3$. Note that the value is *not* the integral under the blue curve, it is the fraction of lost capability that is recovered. Lastly, the green graph shows the effect of an option j_2 that results in avoidance of the threat completely, in which case full capability is retained, and $W_{i,j_2} = 1$.

Figure 3.1. Calculating Baseline and Option Resilience



- Several potential portfolios of options $OP_1, \ldots, OP_s$ may be considered; where we treat each portfolio OP_k as a vector consisting of *m* components $OP_{k,1}, \ldots, OP_{k,m}$ with $OP_{k,j} = 1$ if option O_j is part of portfolio *k*, and 0 otherwise. Then the cost of portfolio *k* is $OPC_k = \sum_{j=1}^{m} OP_{k,j} C_j$. For simplicity, we will let OP_0 denote the portfolio containing no options; that is, only the ability of the baseline to recover capability is considered.

We let $R_a(OP_k)$ denote the resilience of a system for a single DOTMLPF element *e* with the addition of the options (possibly none) in portfolio *k*. It is calculated as follows for the baseline portfolio OP_0: $R_e(OP_0) = \dfrac{\sum_{i=1}^{n} P_i\left(1 - I_i\left(1 - W_{i,0}\right)\right)}{\sum_{i=1}^{n} P_i}$. To parse the equation, each term in the sum in the numerator is the amount of capability retained after the impact due to the adverse events in a test case that is recovered by the baseline system, weighted by the weights associated to each test case. Thus, the numerator is the weighted average of the capability retained in each test case. This sum is scaled by the sum of the weights to get a resilience value between 0 and 1.

For a general portfolio, we have a challenge in determining how to combine one or more options acting against the adverse events in a particular test case, since the impacts of the options may be correlated. The most optimistic assessment is that they all act independently and the recovered capability is calculated as a product. The most pessimistic assessment is that their combined effect is equal to the maximum of the effects of the individual options in the portfolio. We therefore define two resilience functions, R_e^{opt} for the optimistic resilience function and R_e^{pes} or the pessimistic resilience function for element *e*. For a portfolio OP_k, they are defined by

$$R_e^{opt}\left(OP_k\right) = \frac{\sum_{i=1}^{n} P_i \left(1 - I_i\left(1 - W_{i,0}\right)\prod_{j=1}^{m}\left(1 - W_{i,j}P_{k,j}\right)\right)}{\sum_{i=1}^{n} P_i} \text{ and}$$

$$R_e^{pes}\left(OP_k\right) = \frac{\sum_{i=1}^{n} P_i \left(1 - I_i\left(1 - W_{i,0}\right)\left(1 - \max_{1\le j\le n} W_{i,j}P_{k,j}\right)\right)}{\sum_{i=1}^{n} P_i}.$$ [16]

For the DOTPF elements we analyzed, we defined capability metrics for each element:[17]

- *Doctrine*: Metric is whether tactics, techniques, or procedures are available to address a given adverse event against a system and their quality.
- *Organization*: Metric is the fraction of time that effective (that is, above minimum mission capability) command and control for the system is provided in the presence of an adverse event.
- *Training*: Metric is whether personnel are trained to act in a resilient manner against a particular adverse event and the quality of the training.
- *Personnel*: Metric is the fraction of time that sufficient numbers of qualified personnel are available to keep a system operational during an adverse event.
- *Facilities*: Metric is the fraction of time that the capabilities provided by the system's facilities are available during an adverse event.

This is a limited list of metrics; the analysis would include more in a larger system assessment. A spanning test set of potential collections of adverse events should be gathered based on literature reviews, subject-matter expert reviews, and supplementation. A useful preliminary source for such a review can be found in many texts on business continuity and risk management. Of particular note, the Supply Chain Risk Leadership Council has published a useful initial list in their compilation of best practices.[18] Similarly, the Federal Financial Institutions Examination Council publishes a business continuity guide for regulated firms, which has an appendix with a list.[19] For the assessment of resilience, a compilation of these that are applicable generally is as follows:

---

[16] For the remainder of this section, $R_e\left(OP_k\right)$ implies one of either $R_e^{opt}\left(OP_k\right)$ or $R_e^{pes}\left(OP_k\right)$

[17] These metrics were developed for our purposes and can be expanded or modified as needed. For any metrics used in the resilience calculations, the questions raised in the MITRE study for determining the quality of a potential metric should be considered.

[18] Supply Chain Risk Leadership Council, 2011.

[19] Federal Financial Institutions Examination Council, 2008.

- *Natural disasters*: fire, floods and other water damage, severe weather, air contaminants, hazardous spill, pandemics
- *Technical disasters*: power failure, equipment and software failure, transportation system disruptions, water system disruptions, and communications failure with any of: customers, employees, vendors or service providers
- *External risks categories*: sabotage/terrorism/crime/war, government/political risks, labor availability, and technological trends
- *Other party risks*: production problems, financial issues (of suppliers), management risks, upstream supply risks (subcontractors and their sources)
- *Internal risks*: operational risks (process issues, capacity vs. demand, quality), demand variability, skills availability, planning failures, and testing failures
- *Malicious Behaviors*: fraud/theft/blackmail, sabotage, vandalism/looting, terrorism, kinetic, hacking, insider threat, or other attacks
- *Emerging risks*: climate change, social inequality, increased populations, urban vs. rural population, mega cities and ageing populations, dependence on IT.

For adversary-susceptible systems, such as computer or military systems that may be targeted in an engagement, a variety of potential adversary actions should be considered.

Once a spanning test set of collections of adverse events is compiled for the system under consideration, the list is restricted to those applicable to the specific system. The review should use several triggers to suggest inclusion in the final list; past occurrence, proximity, and exposure to the consequences. These triggers should be used to ensure that no relevant risk is ignored. If the risk has occurred to the system, location, or domain under consideration before, it should certainly be included. For some risks, this should be based on proximity to potential causes. For example, any location in a hurricane-exposed region should include hurricanes, and almost any region should list earthquakes, though the probability and magnitude will differ by location. Lastly, the list should include any non-localized risk, such as economic downturns, shortage of supplies, or similar events, if there is an aspect of the system that is exposed to the consequences of the event. Typically, peacetime adverse events can be assessed in terms of absolute probabilities, whereas the weights of adverse events during wartime would be a relative measure, because the adversaries' choice of adverse events is not a static probability but instead depends on an interaction with our systems.

There are methods that have been helpful in reducing the complexity of assessing baseline resilience. Events can typically be categorized in terms of the types of impacts they can cause. Using traditional risk analysis methods,[20] events are mapped to the hazards they cause and the consequences possible. This allows for events with very different characteristics to be viewed as

[20] For military systems, presumably much of this work has been accomplished based on MIL-STD-882E. The required Preliminary Hazard List (Task 201) should contain a list of risks evaluated, and Task 202 should have performed much of what is required for this step. Not all components of a system that we are concerned with from a resilience standpoint are necessarily included in these assessments, so supplemental work will presumably be needed.

similar in terms of how they affect the system, reducing the number of distinct adverse event-impact discussions needed.

Interdependencies and Overall Resilience

The above calculation of element resilience assumes that the different DOTMLPF-P elements are independent of one another, when generally this is not the case. Strong training in resilience potentially results in a resilient organization, strong doctrine results in well-trained personnel, and so forth. In addition, elements contribute differently to an overall notion of resilience, and those contributions may change depending on whether day-to-day operations or those during a crisis are considered. To handle the first point, we performed a nodal analysis of the elements, determining linkages and the strengths of their influence. Letting $L_{a,b}$ denote the level of influence of element *a* on element *b*, with $L_{a,a} = 1$, we produce an influenced resilience $R_e^{\inf}\left(OP_k\right) = \frac{\sum_{b \in \text{Elements}} L_{b,e} R_b\left(P_k\right)}{\sum_{b \in \text{Elements}} L_{b,e}}$, with the denominator normalizing the weights of the contributions of all of the elements to 1.

Finally, we map the influenced resiliencies of the elements into a single resilience number that is posture-dependent. For our work, we consider the resilience of day-to-day operations and the resilience of operations during a crisis, with different weightings on the elements for each posture. Resilient day-to-day operations maintain required capability levels in a mostly unstressed environment, with an emphasis on developing and maintaining processes for when a conflict breaks out. In a crisis, the ability to execute and maintain operations in a stressed environment means that the resilience of personnel is more important than the resilience of doctrine during the crisis. Letting $A_{e,p}$ denote the element weighting of element *e* in posture *p*, with the added constraint that $\sum_{e \in \text{Elements}} A_{e,p} = 1$ for each posture, the overall resilience for a posture *p* and option portfolio OP_k is a weighted sum of the influenced resiliencies for each element: $R_p\left(OP_k\right) = \sum_{e \in \text{Elements}} A_{e,p} R_e^{\inf}\left(OP_k\right)$.

Case Study Example

To illustrate how the method works and to exercise RAPAPORT, the tool we developed[21] to present results from the resilience calculations, we performed a case study that looked at a space architecture to evaluate resilience against three test cases corresponding to single threats, a

---

[21] More details regarding the operation of RAPAPORT are in Chapter Four.

kinetic anti-satellite (ASAT) threat, an uplink jamming threat, and a laser blinding or dazzling attack against satellites. For simplicity, we weight the threats and their impacts against each element equally, $W_i = 1$ for $i = 1, 2, 3$. The explanations and justifications for our weighting and assessments of the system's baseline capability and the improvements in resilience due to options are given in a separate paper.[22] The options considered in the case study are in Table 3.1 along with the element of resilience that they influence.

Table 3.1. Options Considered in Case Study

DOTMLPF Element	Description
Doctrine	Develop tactics for likely counterspace threats in advance of their deployment.
Doctrine	Develop a more timely anomaly resolution process (e.g. first rule out attack and space weather, orbital debris).
Organization	Transfer space order of battle responsibilities from the National Air and Space Intelligence Center to Joint Space Operations Center Intelligence Surveillance and Reconnaissance Division (JSpOC ISRD).
Organization	Task JSpOC ISRD with providing threat advisories and providing indications and warning (I&W).
Organization	Introduce defensive space control officer position (or space protection lead) at Space Operations Squadron and Space Warning (SOPS/SWS), Group, and/or Wing levels.
Organization	Develop rules of engagement and authorize lowest levels of command to respond, with higher echelons exercising command by negation (space mission–dependent).
Organization	Consider developing a common operating system, e.g.. Multi-Mission Satellite Operating Center (MMSOC).
Organization	Increase the number of available ground sites by leveraging allied and commercial command and control capabilities (space mission–dependent).
Organization	Determine and implement best means for JSpOC ISRD to provide daily threat advisories and I&W information to Wing INTEL and/or SOPS.
Organization	Review/modify information sanitization procedures/protocols for granting temporary clearances based on operational needs (e.g., Coal Warfighter).
Training	Update training process to include response to adversary counterspace actions.
Training	For current exercises (e.g., Red Flag), bring space training goals.
Training	Develop new space exercises in which space operators respond to adversary counterspace actions.
Training	Ensure space training (including Blue space and Red counter-space) for intelligence officers assigned to JSpOC and to lower-echelon space units.
Training	Enable cross-training for crew positions within a SOPS.
Personnel	Develop cadre of government civilians with knowledge of U.S. and foreign space capabilities and assign them to JSpOC ISRD.
Personnel	Consider alternative manning (e.g., Reserve, Guard, or civilian) to increase average experience level and reduce training demand.

[22] McLeod et al., 2016.

DOTMLPF Element	Description
Personnel	Review qualifications to become space operators, taking into account that space is now congested, contested, and competitive (consider need to require science, technology, engineering, or math degree and/or aptitude)
Personnel	Ensure that career progression and necessary technical skill acquisition and maintenance are effectively synchronized
Personnel	Use more government civilian personnel and/or lengthen military assignments to increase average experience level and technical capability within SOPS and the JSpOC.
Facilities	Ensure that mobile units for strategic missions are appropriately maintained/available.

Our assessments of baseline capability of the current system against these threats and the improvements due to adding options are derived from input from subject-matter experts. Although the tool allows for considerable fidelity when assessing the baseline and options capability against a threat, we found that six-level characterization of capability (None, Low, Low/Medium, Medium, Medium/High, and High) was sufficient for our needs. This color coding along with the numeric values associated with each level is shown in Figure 3.2.

Figure 3.2. Color Coding for Baseline and Options Capability

Color Key:	None (0)	Low (0.1)	Low/Medium (0.25)	Medium (0.5)	Medium/High (0.75)	High (1)
Baseline Meaning	no capability on threat impact	little capability on threat impact	minimal capability on impact	noticeable capability on threat impact	high capability on threat impact	very significant capability on threat impact
Option Meaning	no added capability on threat impact	little added capability on threat impact	minimal added capability on impact	noticeable added capability on threat impact	high added capability on threat impact	very significant added capability on threat impact

In Figures 3.3a–3.3e, we show the assessment of the baseline and options against each of the three threats in each of the elements under consideration (DOTPF). The level of capability of the baseline represents the already-existing resilience against a threat. For the evaluation of the options, it should be noted that the colors are used to denote the effect of the option above and beyond any resilience due to the baseline alone; accordingly, the option colors and the values they represent may be inferior to those of the baseline. Again, we refer to the main project document for the justification behind these assessments. Note that, for example, in Figure 3.3e, since these threats have no direct impact on the facilities of the system, the baseline assessment of capability against these threats is the highest possible.

Figure 3.3a. Assessment of Baseline and Options Capability Against Each Threat, by Element—Doctrine

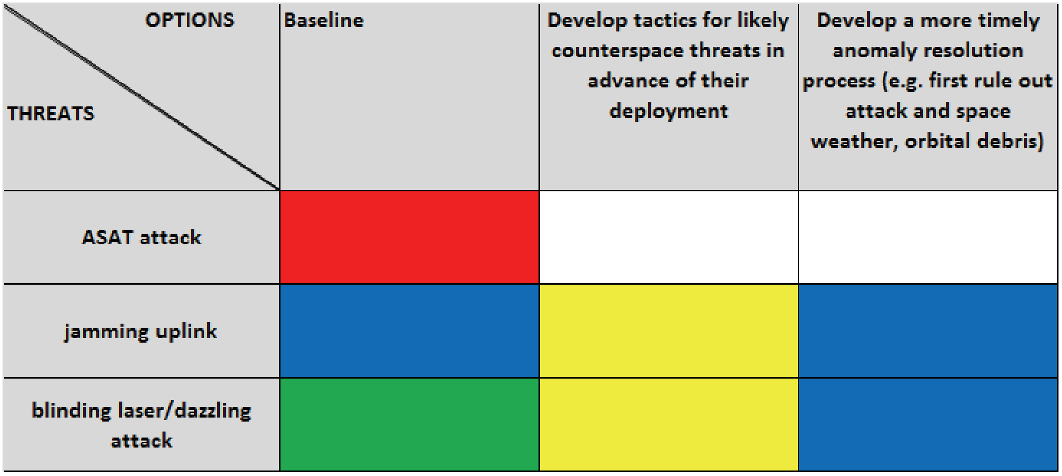


Figure 3.3b. Assessment of Baseline and Options Capability Against Each Threat, by Element—Organization

THREATS / OPTIONS	Baseline	Transfer space order of battle responsibilities from NASIC to JSpOC ISRD	Task JSpOC ISRD with providing threat advisories, providing indications and warning (I&W)	Introduce defensive space control officer position (or space protection lead) at SOPS/SWS, Group, and/or Wing levels	Develop ROE and authorize lowest levels of command to respond, with higher echelons exercising command by negation (space mission dependent)	Consider developing a common operating system, e.g. MMSOC	Increase the number of available ground sites by leveraging allied and commercial C2 capabilities (space mission dependent)	Determine & Implement best means for JSpOC ISRD to provide daily threat advisories and I&W information to Wing INTEL and/or SOPS	Review/modify information sanitization procedures/protocols for granting temporary clearances based on operational needs (e.g., Coal Warfighter)
ASAT attack									
jamming uplink									
blinding laser/dazzling attack									

Figure 3.3c. Assessment of Baseline and Options Capability Against Each Threat, by Element—Training

THREATS / OPTIONS	Baseline	Update training process to include response to adversary counterspace actions	For current exercises (e.g. Red Flag), bring space training goals	Develop new space exercises in which space operators respond to adversary counterspace actions	Ensure space training (including Blue space and Red counter-space) for intelligence officers assigned to JSpOC and to lower echelon space units	Enable cross-training for crew positions within a SOPS
ASAT attack						
jamming uplink						
blinding laser/dazzling attack						

Figure 3.3d. Assessment of Baseline and Options Capability Against Each Threat, by Element—Personnel

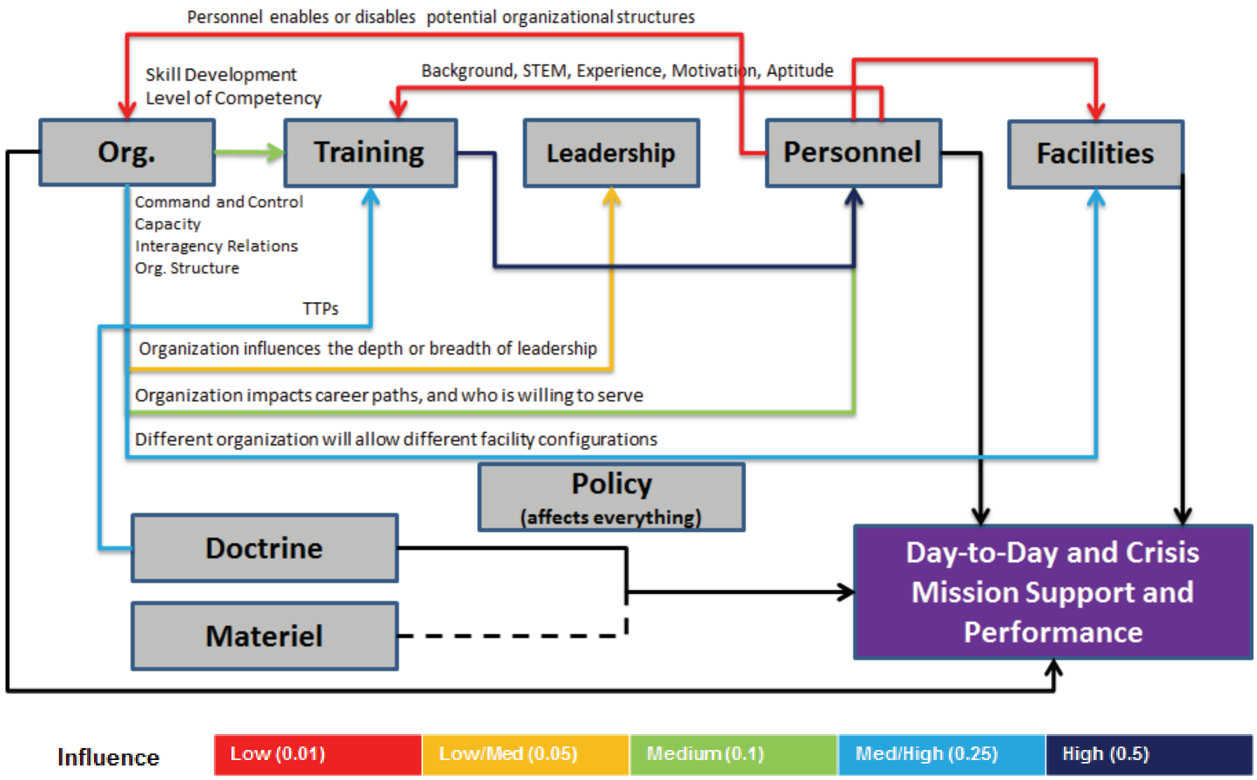
THREATS \ OPTIONS	Baseline	Develop cadre of government civilians with knowledge of U.S. and foreign space capabilities and assign them to JSpOC ISRD	Consider alternative manning (e.g., Reserve, Guard, or civilian) to increase average experience level and reduce training demand	Review qualifications to become space operators, taking into account that space is now congested, contested, and competitive (consider need to require STEM degree and/or aptitude)	Ensure that career progression and necessary technical skill acquisition and maintenance are effectively synchronized	Use more government civilian personnel and/or lengthen military assignments to increase average experience level and technical capability within SOPS and the JSpOC
ASAT attack						
jamming uplink						
blinding laser/dazzling attack						

Figure 3.3e. Assessment of Baseline and Options Capability Against Each Threat, by Element—Facilities

OPTIONS / THREATS	Baseline	Ensure mobile units for strategic missions are appropriately maintained/available
ASAT attack		
jamming uplink		
blinding laser/dazzling attack		

The evaluations above help to determine the resilience of each DOTPF element. However, these elements are interconnected; an improvement in the resilience of training would also improve the resilience of personnel (and vice versa, although with a smaller influence). To determine the influenced resiliencies of each element, we used in-house subject-matter experts to determine the influences of each element on the others. In Figure 3.4, we show in a directed graph the linkages we established between the different elements under consideration for our nodal analysis, with arcs going from influencing element to influenced and color coding of the linkages denoting the strength of the influence. In addition, we note that the elements of doctrine, organization, personnel, and facilities contribute to the overall resilience of both day-to-day and crisis mission support and performance, providing our two postures for evaluating overall resilience. Note that we do not weight the resilience of training as contributing directly to the overall resilience of day-to-day and crisis missions support and performance, as training does not directly affect operations, rather it has a secondary effect on the other elements. In other words, $A_{Training,p} = 0$ for both postures *p*. Based on our discussions with subject-matter experts, for day-to-day operations, we weight the influenced resilience of these elements equally (25 percent each), whereas in a crisis, we place a higher priority on the resilience of the personnel relative to the other elements, as their quality is key to mission success during a crisis, more so than, say, doctrine or organization (15 percent doctrine, 10 percent organization, 50 percent personnel, and 25 percent facilities). We note that the dependencies and weights we assigned are preliminary and should be refined by appropriate government subject-matter experts, since they have more insights into the inner workings of the different DOTMLPF elements that we evaluated.

Figure 3.4. Directed Graph Representation of DOTMLPF-P Resilience Interdependencies



NOTE: TTPs = tactics, techniques, and procedures.

For our portfolios of options, we consider the portfolio consisting of all of the options, as well as portfolios corresponding to all of the options for each element under consideration. Note that options may potentially improve capability in more than one element, but for this example we keep them separate. The results from the resilience calculations are shown in Figure 3.5, which shows both the uninfluenced and influenced values of resilience and the overall day-to-day and crisis resilience. For the results, we assume the optimistic combination of option effects on capability. The color coding in the table corresponds to the color key for the baseline and options shown in Figure 3.2, with the largest color threshold less than or equal to the value setting the color (e.g., 0.45 is greater than 0.25 and less than 0.5, so yellow for Low/Medium). As an example calculation, although the uninfluenced resilience of the facilities is equal to 1, because the element resilience of some of the elements that influence facilities resilience are less than 1, the influenced facilities resilience is also less than 1. Tracking the overall resilience calculation for the baseline case, for the overall day-to-day resilience the value is the average of the doctrine, organization, personnel, and facilities influenced resilience values $(0.45+0.33+0.23+0.86)/4=0.47$), with the overall crisis resilience slightly lower, as personnel resilience has a greater impact and is lower (0.23) than average. As the chart shows, as expected, each portfolio consisting of all of the options for one DOTPF element improves the resilience score for that element alone.

To walk through a sample calculation from Figure 3.5, consider the All Doctrine portfolio (the portfolio containing all options to improve the doctrine aspect of resilience) relative to the baseline (the third column in Figure 3.5). This is the portfolio consisting of the first two options in Table 3.1, "Develop tactics for likely counterspace threats in advance of their deployment" and "Develop a more timely anomaly resolution process (e.g., first rule out attack and space weather, orbital debris)." Using the assessments from Figure 3.3a, the resilience against the ASAT attack is unchanged by the doctrine options (0.1), the resilience against the jamming attack increases from 0.75 to $1-(1-0.75)(1-0.25)(1-0.75)=0.953125$, and the resilience against the blinding laser/dazzling attack increases from 0.5 to $1-(1-0.5)(1-0.25)(1-0.75)=0.90625$, resulting in an uninfluenced doctrine resilience of $(0.1+0.953125+0.90625)/3=0.653125$. Had we used the pessimistic calculation for resilience, the resilience against the jamming attack would have increased from 0.75 to $1-(1-0.75)(1-0.75)=0.9375$, and the resilience against the blinding laser/dazzling attack would have increased from 0.5 to $1-(1-0.5)(1-0.75)=0.875$, resulting in an uninfluenced doctrine resilience of $(0.1+0.9375+0.875)/3=0.6375$. In the nodal analysis shown in Figure 3.4, doctrine influences training at a medium-high level (0.25), and we weight training's influence on itself at 1, which when scaled down by the sum of the weights (1.25) results in a relative weighting of 0.8 for training and 0.2 for doctrine, resulting in an influenced training resilience of $0.8\times0.17+0.2\times0.65=0.27$.

Figure 3.5. Results from Optimistic Resilience Calculations

Uninfluenced Resil.	Baseline	Everything	All Doctrine	All Organization	All Training	All Personnel	All Facilities
Doctrine	0.45	0.65	0.65	0.45	0.45	0.45	0.45
Organization	0.33	0.85	0.33	0.85	0.33	0.33	0.33
Training	0.17	0.72	0.17	0.17	0.72	0.17	0.17
Personnel	0.25	0.69	0.25	0.25	0.25	0.69	0.25
Facilities	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Influenced Resil.	**Baseline**	**Everything**	**All Doctrine**	**All Organization**	**All Training**	**All Personnel**	**All Facilities**
Doctrine	0.45	0.65	0.65	0.45	0.45	0.45	0.45
Organization	0.33	0.85	0.33	0.85	0.33	0.34	0.33
Training	0.23	0.71	0.27	0.27	0.63	0.23	0.23
Personnel	0.23	0.71	0.23	0.26	0.40	0.51	0.23
Facilities	0.86	0.97	0.86	0.96	0.86	0.87	0.86
Overall Resil.	**Baseline**	**Everything**	**All Doctrine**	**All Organization**	**All Training**	**All Personnel**	**All Facilities**
Day-to-Day	0.47	0.80	0.52	0.63	0.51	0.54	0.47
Crisis*	0.43	0.78	0.46	0.52	0.52	0.57	0.43

In Chapter Four, we will describe some of the other potential outputs in greater detail. For example, with cost data for the options, the cost of portfolios can be determined and then plotted against overall resilience to find an efficient frontier of portfolios. Similarly, the tool has the capability to do marginal analysis on a portfolio to see whether there is a particular option (or pair of options) that is predominantly driving the results for that portfolio.

In conclusion, we have shown the pedigree of our method derived from other methods in industry to calculate the resilience of a space system, explained how it calculates the resilience of a system enhanced by a portfolio of options, and shown an example of the calculations. The resilience assessment process is not specific to the space resilience task for which it was created and can be used for any U.S. Air Force (or DoD) system, provided that the system and its DOTMLPF-P elements, potential adverse events, options, and their linkages are well understood.

4. The Portfolio Option Reporting Tool

Introduction

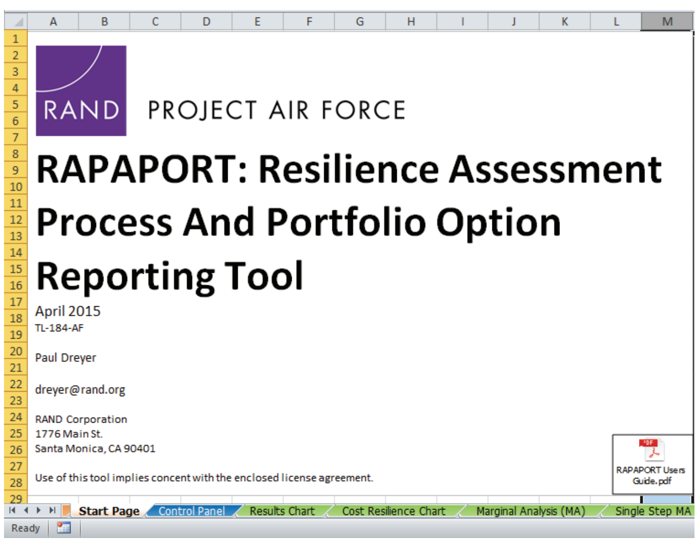
RAPAPORT is implemented as a workbook in Microsoft Excel with a Visual Basic back end to handle calculations and outputs.[23] The capabilities of options against test cases of adverse events (in the tool denoted as Threats for compactness) can be represented either with numeric values or with the color of the cell (which maps back to a particular numeric value). Below, we describe how to set up a resilience assessment process inside the tool and the set of outputs available.

Input Sheets (red tabs)

Start Page

The Start Page sheet (Figure 4.1) appears when the workbook is opened. It contains contact information for the author, copyright information, and a PDF copy of this chapter of the document.

Figure 4.1. Welcome Sheet



[23] RAPAPORT is available at www.rand.org/t/TL184. The tool has been tested in Microsoft Excel 2007 and 2010 for Windows and 2008 for Macs.

Control Panel

The Control Panel sheet is actually both an input and output sheet, consisting of a series of tables for data entry and then the numeric results from the resilience calculations at the bottom of the sheet.

Color Key

The color key (Figure 4.2) is used throughout the workbook to denote levels of capability (Low, Low/Medium, Medium, Medium/High, and High). Unless a cell contains a number between 0 and 1, the value associated to that entry corresponds to the color of the cell. If the cell has no fill (or has a white fill), it is assumed that the value is zero. If other cell colors are used in the assessment tables, the tool will announce an error. Using cell fill colors as the identifier of capability has the added bonus that text can be entered in the cells explaining how the level of capability was determined. If the user decides to use a different set of colors, there is a swap key in the first row in columns J through N. The user can put the desired colors in those cells, click on the Swap Colors button, and the desired colors will become the default colors and will be swapped throughout the entire workbook.

Figure 4.2. Color Key

Baseline and Option Weights

There are two tables that define to what values the colors correspond. There are separate tables for the baseline and the option assessments. (An example Baseline Weights table is shown in Figure 4.3.) The value of a color can change from element to element.

Figure 4.3. Baseline Weights Table

Baseline Weights					
Doctrine	**0.1**	**0.25**	**0.5**	**0.75**	**1**
Organization	**0.1**	**0.25**	**0.5**	**0.75**	**1**
Training	**0.1**	**0.25**	**0.5**	**0.75**	**1**
Personnel	**0.1**	**0.25**	**0.5**	**0.75**	**1**
Facilities	**0.1**	**0.25**	**0.5**	**0.75**	**1**

Link Weights and Linkages

To calculate the influenced element resilience, it is necessary to enter the linkages between the various elements. Link weights are again color coded (using the same color scale as the baseline and option weights), although the values they represent may be different. Below, the link weights row is a table where linkages between influencing element and influenced element can be added.

Each row consists of two element names, with a color in the third column representing the strength of the influence (the text shown in the colored cells in the example above is not necessary). As an example, in Figure 4.4, it is assessed that the DOTMLPF element of Organization influences the element of Personnel at a Medium level and Facilities at a Medium/High level. Accordingly, a change in the resilience of the Organization element would result in a greater influence on Facilities than on Personnel.

Figure 4.4. Link Weights and Element Linkages Table

Link Weights		0.01	0.05	0.1	0.25	0.5

Linkages

Influencer	Influenced	Levels
Doctrine	Training	M/H
Organization	Training	M
Organization	Personnel	M
Organization	Facilities	M/H
Training	Organization	N
Training	Personnel	H
Personnel	Organization	L
Personnel	Training	L
Personnel	Facilities	L

Posture Resilience Element Weights

For each posture under consideration, a different weighting of (influenced) element resilience should be added to the right of the Weightings table as a new column. The entry at the bottom is calculated and will be red or green depending on whether the sum of the weights of the elements is 1 or not. A scatterplot of overall resilience versus cost is one of the output sheets, and the posture that should be shown in that scatterplot should be identified with an asterisk somewhere in the posture name. Also shown in Figure 4.5 is the Run Model button, which causes all of the resilience calculations to be performed.

Figure 4.5. Posture Resilience Element Weights Table

Run Model

Weightings (* appears in scatterplot)	Day-to-Day	Crisis*
Doctrine	25%	15%
Organization	25%	10%
Training	0%	0%
Personnel	25%	50%
Facilities	25%	25%
Total	100%	100%

Cost and Portfolio Option Information

The remainder of the inputs on this worksheet define the options and portfolio compositions (Figure 4.6). In the Options List, each row represents and option and has a description, which element it applies to, the cost and ease of implementation of the option. The cost can be a number, or Low, Medium, or High (or just the first letters, L/M/H). The Cost Category table above the options list gives a corresponding representative cost for each cost category. The Ease to Implement column also takes L/M/H values. Each portfolio should be represented as a column directly to the right of the four columns describing the options, with its name in the top row and its composition described by either 0s and 1s for each option row, depending on whether the option is contained in the portfolio or not. Note, for example, that the Everything portfolio contains all of the first three options, while the All Doctrine portfolio contains only the first two (not all options are shown). The Options Combo Rule above the Options List is either an M or a P, representing [M]aximum or [P]roduct, corresponding to the most pessimistic or optimistic rule, respectively, for combining multiple options against the adverse events in a test case. Options and portfolios can be added or removed by adding or deleting rows (columns) as appropriate.

Figure 4.6. Cost Information, Options List, and Portfolio Composition Table

Cost Category	Representative Cost ($M)
Low	0.05
Medium	2
High	5

Options Combo Rule: P

Options List

		Enter numbers or Low/Med/High		Portfolios Include (0/1)					
Description	Aspect	Cost	Ease to Implement	Everything	All Doctrine	All Organization	All Training	All Personnel	All Facilities
Develop tactics for likely counterspace threats in	Doctrine	L	M	1	1	0	0	0	0
Develop a more timely anomaly resolution process	Doctrine	M	L	1	1	0	0	0	0
Transfer space order of battle responsibilities from	Organization	H	M	1	0	1	0	0	0

Threats Versus Impacts

This table has two columns for each element and one row per test case of adverse events (Figure 4.7). For each test case and element, the weight corresponds to either the probability of the event or its relative importance to the decisionmaker. If a threat is added or removed, it must be removed from the Baseline and Option Assessment by Element sheets described below. The impact corresponds to the decrease of the system's capability (that is, the metric being computed for a given DOTMPLF element) if the events in the test case occur unimpeded (ignoring any potential resilience of the current system to the adverse events). Both values should be between 0 and 1 inclusive. The comments on the Impact columns contain the definitions of the metrics being calculated.

Figure 4.7. Threats Versus Impacts Table

Impacts / THREATS	Doctrine		Organization		Training		Personnel		Facilities	
	Weight	Impact	Weight	Impact	Weight	Impact	Weight	Impact	Weight	Impact
ASAT attack	1	1	1	1	1	1	1	1	1	1
jamming uplink	1	1	1	1	1	1	1	1	1	1
blinding laser/dazzling attack	1	1	1	1	1	1	1	1	1	1

Baseline and Option Assessment by Element (Doctrine, Organization, Training, Personnel, and Facilities Sheets)

There are five input worksheets corresponding to the DOTMLPF-P elements under consideration. The Doctrine sheet is shown in Figure 4.8. On each sheet, all of the threats from the Threats Versus Impacts table must be listed in the same order as rows in the tables on these sheets, while the columns correspond to the options specific to that element. If options are added or removed from the model, the corresponding columns must also be removed from these worksheets. The first column corresponds to the baseline capability of the system against each adverse event, while the names in the column headings must match those in the Options List on the Control Panel sheet exactly. The values in the table correspond to the expected amount of lost capability the current system (or an option) can recover against a particular adverse event. The cell colors in the table can be one of the five in the color key or left unfilled (corresponding to a value of zero). Alternatively, if a numeric value between 0 and 1 is entered into the cell, it will be the value used, regardless of the cell color. The calculator re-colors cells with numeric values in them so that they match the color whose representative value is largest and less than or equal to the numeric value in the cell. So, if the cell in the top-left corner contained the value 0.55, the cell would be recolored green (Medium) while retaining the numeric value to be used in the calculations. If cells contain any text other than a number between 0 and 1, the cell color sets the value.

Figure 4.8. Baseline and Option Assessment for Doctrine Table

OPTIONS / THREATS	Baseline	Develop tactics for likely counterspace threats in advance of their deployment	Develop a more timely anomaly resolution process (e.g. first rule out attack and space weather, orbital debris)
ASAT attack			
jamming uplink			
blinding laser/dazzling attack			

Output Sheets (green tabs)

Control Panel

As shown in Figure 4.9, the outputs on the Control Panel sheet give the element resilience for each portfolio (including the baseline), both influenced and uninfluenced, as well as the overall resilience by posture. The values are color coded using the same color scheme as the color key in the Baseline Weights table. The cost of each portfolio is given as the final row and is used in the Cost Resilience Chart sheet, described momentarily.

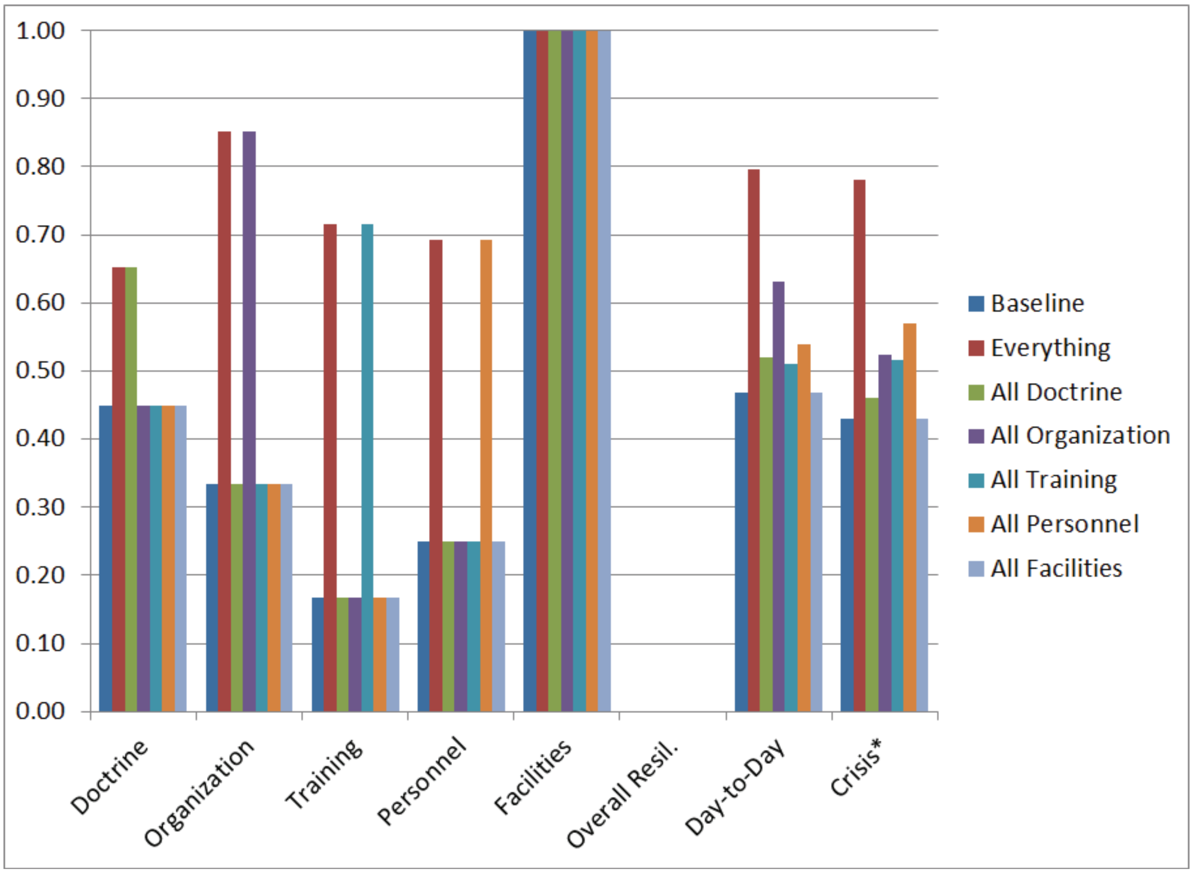
Figure 4.9. Control Panel Outputs

Output							
Uninfluenced Resil.	Baseline	Everything	All Doctrine	All Organization	All Training	All Personnel	All Facilities
Doctrine	0.45	0.65	0.65	0.45	0.45	0.45	0.45
Organization	0.33	0.85	0.33	0.85	0.33	0.33	0.33
Training	0.17	0.72	0.17	0.17	0.72	0.17	0.17
Personnel	0.25	0.69	0.25	0.25	0.25	0.69	0.25
Facilities	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Influenced Resil.	Baseline	Everything	All Doctrine	All Organization	All Training	All Personnel	All Facilities
Doctrine	0.45	0.65	0.65	0.45	0.45	0.45	0.45
Organization	0.33	0.85	0.33	0.85	0.33	0.34	0.33
Training	0.23	0.71	0.27	0.27	0.63	0.23	0.23
Personnel	0.23	0.71	0.23	0.26	0.40	0.51	0.23
Facilities	0.86	0.97	0.86	0.96	0.86	0.87	0.86
Overall Resil.	Baseline	Everything	All Doctrine	All Organization	All Training	All Personnel	All Facilities
Day-to-Day	0.47	0.80	0.52	0.63	0.51	0.54	0.47
Crisis*	0.43	0.78	0.46	0.52	0.52	0.57	0.43
Portfolio Cost	0	44.4	2.05	12.25	14.05	11.05	5

Results Chart

Figure 4.10 has two sets of bar charts: the uninfluenced resilience for each element and portfolio, and the posture-specific overall resilience values for each portfolio, which are weighted sums of the influenced resiliencies for each element.

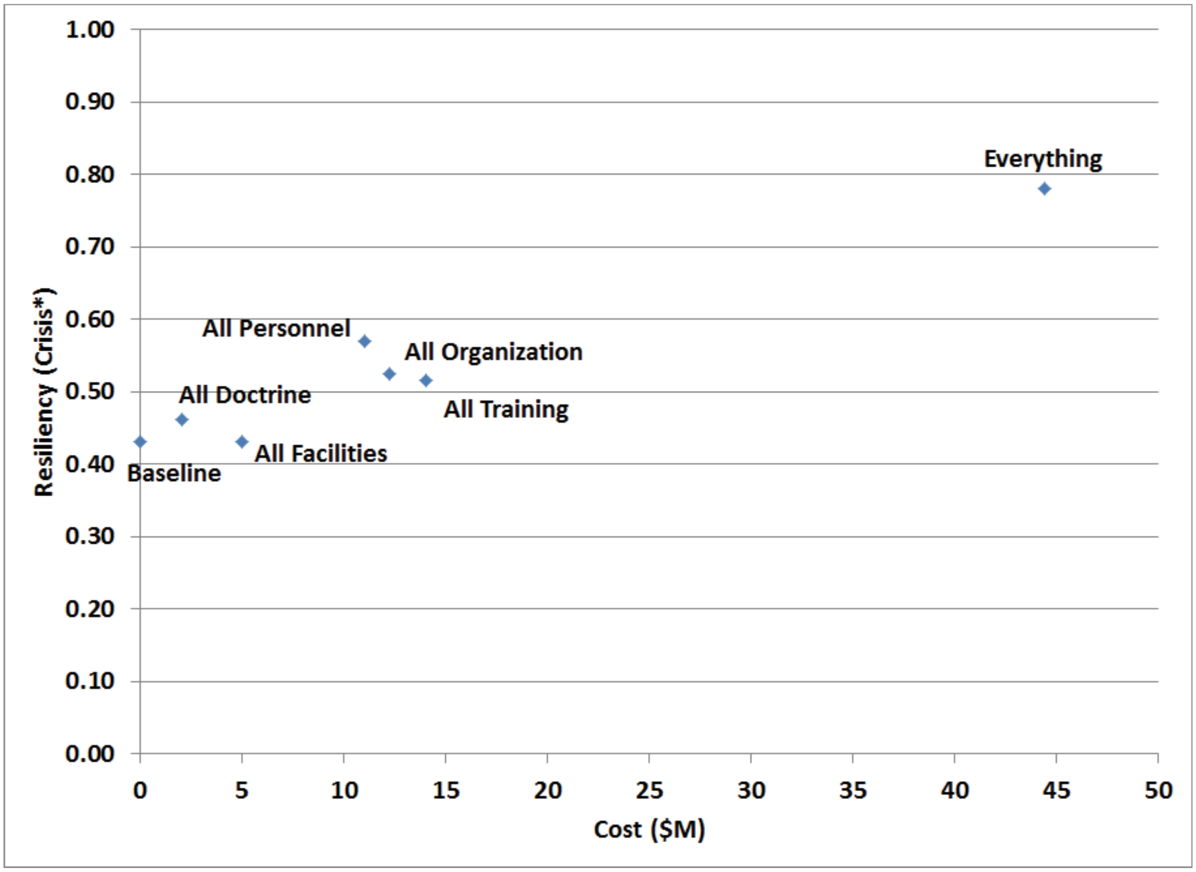
Figure 4.10. Results Chart



Cost Resilience Chart

Figure 4.11 is a scatterplot of portfolio cost versus overall resilience for the Crisis posture.

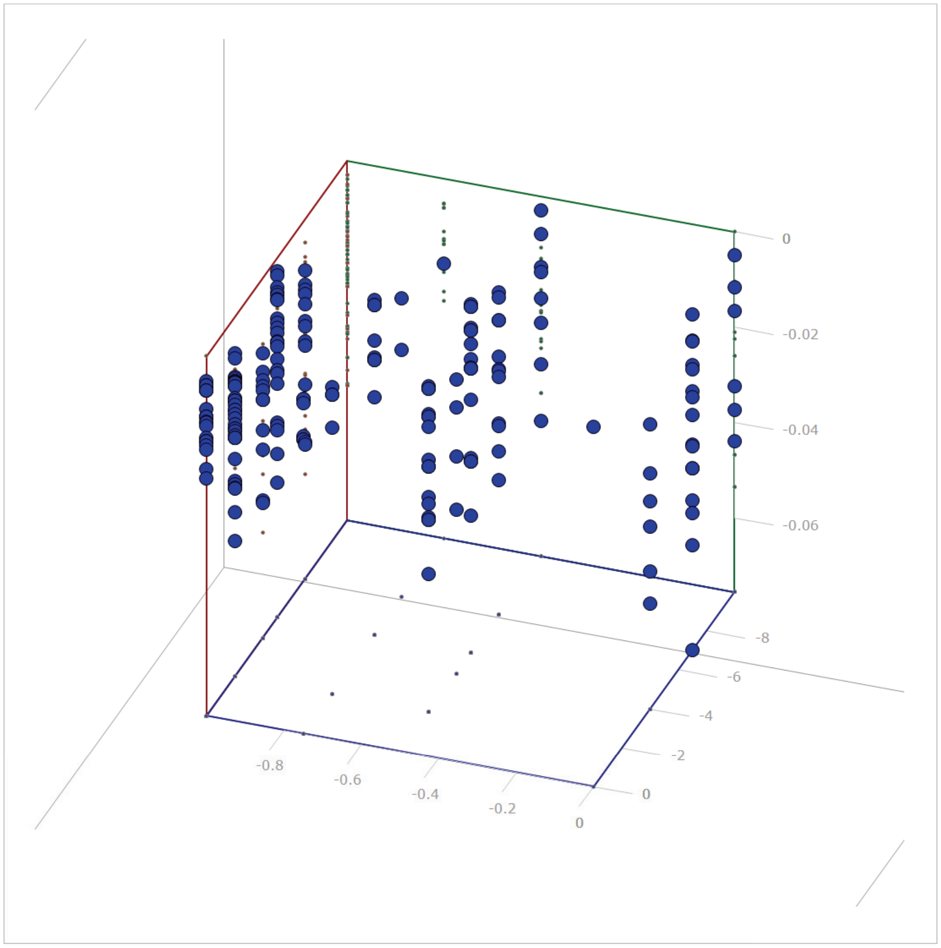
Figure 4.11. Cost Resilience Chart



Marginal Analysis (MA), Single Step MA Plot, Double Step MA Plot

On the Marginal Analysis (MA) sheet is the Run Marginals button. If the button is pressed, the user can select an initial portfolio from which marginal analysis will be performed. In addition, the user can specify whether insertions and/or deletions from the portfolio can be considered, as well as the posture-specific overall resilience value that should be used for comparing portfolios. The tool then considers all portfolios that consist of the initial portfolio plus one or two insertions or deletions of options (as specified by the user) and ranks them by the change to the specified overall resilience value. The portfolios with one and two option changes are in separate tables, and each table also notes the cost deltas as well as deltas in ease of implementation. The Single Step MA Plot and Double Step MA Plot sheets have three-dimensional scatter plots with cost and ease of implementation deltas as the x- and y-axis, and the resilience delta as the z-axis. A sample three-dimensional scatter plot result from the marginal analysis is shown in Figure 4.12.

Figure 4.12. Sample Marginal Analysis 3-D Scatter Plot



References

Air Force Space Command, *Resiliency and Disaggregated Space Architectures*, white paper, 2013. As of September 23, 2015: http://www.afspc.af.mil/shared/media/document/AFD-130821-034.pdf

Alberts, David S., *The Agility Advantage: A Survival Guide for Complex Enterprises and Endeavors*, DoD Command Control Research Program, 2011. As of September 23, 2015: http://www.dodccrp.org/files/agility_advantage/Agility_Advantage_Book.pdf

Brtis John, "A Framework for Thinking About Resiliency," briefing, AFLCMC MA/Cyber Resilience Working Group, January 16, 2013.

Burch R., "Measures of Resilience for Space Systems," presentation to the National Defense Industrial Association Resilience Forum, 2013, As of September 23, 2015: http://www.ndia.org/Divisions/Divisions/Space/Documents/Space_forum-Boeing-NDIA-Resilience-Forum-081413-RevA.pdf

Davis, Paul K., *Analysis to Inform Defense Planning Despite Austerity*, Santa Monica, Calif.: RAND Corporation, RR-482, 2014. As of September 23, 2015: http://www.rand.org/pubs/research_reports/RR482.html

Edlund, Gregory, "Space Systems Resiliency: Definition, Measurement, and Application," presentation to Air Force Space Command, 2013. As of September 23, 2015: http://www.ndia.org/Divisions/Divisions/Space/Documents/NDIA%20Resiliency%20Update_NGAS13-1829_091613.pdf, 2013

Federal Financial Institutions Examination Council, *Business Continuity Planning*, 2008. As of September 23, 2015: http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

Langeland, Krista S., David Manheim, Gary McLeod, and George Nacouzi, *How Civil Institutions Build Resiliency: Organizational Practices Derived from Academic Literature and Case Studies*, Santa Monica, Calif.: RAND Corporation, RR-1246-AF, 2016. As of April 2016: http://www.rand.org/pubs/research_reports/RR1246.html

Lockheed Martin, "NDIA Forum on Space Resilience: Space Resiliency Study," presentation, August 14, 2013. As of September 23, 2015: http://www.ndia.org/Divisions/Divisions/Space/Documents/Space_forum_LM-Resiliency-Study-Final.pdf

Long, Andrew, "Risk-Based Resiliency Assessment Framework: Achieving Resilient U.S. Space Architectures," presentation, October 2012. As of September 23, 2015: http://www.dtic.mil/ndia/2012system/ttrack314833.pdf

McLeod, Gary, George Nacouzi, Paul Dreyer, Mel Eisman, Myron Hura, Krista S. Langeland, David Manheim, and Geoffrey Torrington, *Enhancing Space Resilience Through Non-Materiel Means*, Santa Monica, Calif.: RAND Corporation, RR-1067-AF, 2016. As of April 2016: http://www.rand.org/pubs/research_reports/RR1067.html

Supply Chain Risk Leadership Council, *Compilation of Best Practices*, 2011. As of September 23, 2015: http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final%5B1%5D.pdf

Task Group SAS-085, *C2 Agility*, STO Technical Report STO-TR-SAS-085, 2014. As of September 23, 2015: http://dodccrp.org/sas-085/sas-085_report_final.pdf

U.S. Department of Defense, *Fact Sheet: Resilience of Space Capabilities*, 2011. As of September 23, 2015: http://www.defense.gov/Portals/1/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf

U.S. Department of Defense, *Standard Practice: System Safety*, MIL-STD-882E, May 2012. As of September 23, 2015: available at http://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=36027

U.S. Department of Defense, Acquisition, Technology, and Logistics, *Risk Management Guide for DOD Acquisition*, Sixth Edition. August, 2006.

The White House, *National Space Policy of the United States of America*, 2010. As of September 23, 2015: http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf

Wilson, Kevin, John Fujita, and Todd Nygren, *Architecting and Analysis Framework for Resilient and Affordable Systems*, Aerospace Report TOR-2014-00201, 2013, not available to the general public.

RAND PROJECT AIR FORCE

www.rand.org

$21.00

ISBN-10 0-8330-9209-X
ISBN-13 978-0-8330-9209-0

52100

9 780833 092090

RR-1169-AF